

PatchLink Update Server v6.0.1

User Manual



1.	PatchLink Update Overview	3
2.	What's new with PatchLink Update version 6.0?	21
3.	Getting Started	23
4.	PatchLink Update Home Page	34
5.	Vulnerabilities	45
6.	Inventory	58
7.	Packages	66
8.	Creating and Editing Packages: Package Editor Wizard	82
9.	Deploying Packages: Schedule Deployment Wizard	97
10.	Computers	117
11.	Groups	171
12.	Add a Group Wizard	204
13.	Edit a Group Wizard	211
14.	Users	218
15.	Reports	223
16.	Create a User Wizard	232
17.	Add a User Wizard	236
18.	Edit a User Wizard	240
19.	Add a Role Wizard	243
20.	Edit a Role Wizard	249
21.	Options	255
22.	Add a Policy Wizard	270
23.	Edit a Policy Wizard	272
24.	Hardening the PLUS	274
25.	PLUS Reference	276
26.	Programmer's Reference	278
27.	Glossary	288
28.	Revision History	293

1. PatchLink Update Overview

During the final step of the Update Server installation, all Vulnerability Fixes in the PatchLink archive* with the designation *Critical* are downloaded to your PatchLink Server. Other Fixes are listed and available for you to download at any time. When your first Vulnerability replication is complete, the next step is to install Update Agent software on your client computers.

The PatchLink Update Agent scans the host computer and compiles information on operating system, software, hardware, and services on that machine. The results of the scan are returned to the Update Server and can be viewed at any time in the Inventory section of the product, even if a workstation is disconnected from your network. Based on this information, Vulnerability Fixes are determined to be applicable or not to each computer. If applicable, the Agents perform another scan using the patch fingerprints incorporated into each Vulnerability Fix to determine the host computer's patch status in relation to that Fix. Once patch status is established, the PatchLink Administrator can deploy the desired fixes to each computer on the network.

PLEASE NOTE: As recommended with all patches, you should first deploy the patch within your test environment before rolling it out into production.

Patch deployment is simple. Use the Vulnerability detail view to see the list of computers that are not patched. Next, select the computers that should receive the patch and schedule the date and time for the deployment to occur. Once a deployment has been scheduled, the detail view shows you the status of the update - how many computers are downloading the patch, how many completed successfully, and delivery error codes in the event of an unsuccessful deployment.

*By default, only Vulnerability Fixes for the Microsoft Windows OS are downloaded. If your Sales agreement includes other operating systems, you will receive additional downloads.

Once installed, your PatchLink Update Server stays current with the latest patches and fixes by daily communication with the PatchLink Host Server via its subscription connection. When a newly released patch matches your stored network profile, you receive a proactive email notification and the new Vulnerability appears on the Update Server with the description and business impact as well as the list of computers that require it. At this time you can choose to deploy the patch or disregard it.

1.1 The Plus Server has the following main components:

Agents: are installed on every computer you wish to manage under PatchLink. They perform detection scans which allow the Update Server to determine security holes and other vulnerabilities. The Agent is then capable of implementing corrective actions received from the Plus Server. In most cases, the agent operates silently, without any direct intervention from the end user. However, the Plus Server also allows the administrator to provide active feedback for those actions that require user input.

The Plus Server is a collection of interacting services, including executable programs, a Web server and a database server, that lies at the heart of the Patchlink system. It coordinates the flow of information to and from individual computers and stores the results in the Patchlink database. The Patchlink Server components operate quietly in the background, without any direct intervention from the administrator.

Patchlink Distribution Point Servers (DPS) increase the efficiency of the system. Instead of forcing each networked computer to directly access the Plus Server, **DPS** spreads the burden. Dozens of Agents can point to a **DPS** for downloads, which in turn makes only a single request of the server. A **DPS** does not need to be a dedicated computer – the software can be installed on any windows client. As soon as you deploy a **DPS**, you can then deploy clients that will connect thru that **DPS** module.

FastPatch is a utility which allows an agent to dynamically locate its closest distribution point, using TraceRoute, enabling mobile computers to be patched with maximal bandwidth efficiency.

The Patchlink Web Console ties all these components together to provide a system-wide view of all the computers on your network, along with their vulnerabilities and suggested remedies. The Patchlink Web Console allows an authorized user to quickly and simply distribute fixes to each computer that needs them without impacting any other networked computers. The Patchlink Web Console can be run on any computer in your network regardless of platform.

The PatchLink Update Server (PLUS) provides a complete solution for proactive reporting, patching and updating of your network. The product includes:

- A subscription service that keeps your PLUS up to date with the latest available Vulnerabilities and their corresponding Packages.
- Using the Detection Agents throughout your network, PLUS will quickly give you a detailed analysis of these fingerprints and signatures. You will quickly be able to determine the patch status of your computers.
- Based on the results of the analysis, you can easily create Package deployments to the computers that need them. Deployments are carried out by the Deployment Agents.
- With this extensive detection mechanism, a comprehensive Inventory system is also available. You will be able to detect what operating systems, software, hardware, device drivers and services are installed on your computers.
- PLUS features a new enterprise-wide agent distribution mechanism called the **Agent Management Center**. Through the use of Deployment (Client) Agents, Package Editor, and the Agent Management Center, you can securely send software, documentation, scripts (SW, HW and Services) or any other content across your network; from small Intranets to huge Extranets, or even the Internet itself.
- **System Groups** can now be manually or automatically created according to the criteria that you establish whether by Active Directory Organizational Units (OU's), NT or Active Directory Domains, LDAP OU's, IP address ranges or geographical regions as well as the default operating system groups. With this feature, you may:
 - View the Vulnerability Analysis based solely on the group membership.
 - View the **Inventory** based on the group membership.
 - **Deploy** patch files (or any other packages) to the entire group. The group's membership can be changed at the start of the deployment to allow the administrator complete versatility in deploying patches. After the deployment is initiated, the members of the group are given the patch packages as their agents check-in with the PLUS server.
 - **Lock** a group for a set of vulnerabilities, software inventory, hardware inventory, or service inventory.
 - Set a **Mandatory Baseline** for a group, so that if the compliancy analysis of vulnerabilities for a group member results in not being patched, the computer will automatically have the vulnerability package deployed to it.

- Customize the group's computer member's behavior based on the group's **Agent Policy Set** (Agent Polling Interval and Hours of Operation). An easy mechanism to allow a group's computer members to act in a specific way while not affecting the other computers registered to the system.
- PLUS contains a complete role-based security layer. A role determines what rights a user has to perform PLUS functionality to the computers and groups of computers the role is assigned to. PLUS contains 4 role templates to assist PLUS Administrators in designing security for the many users of your PLUS System.
- PLUS provides multi-platform support for the following operating systems:

Vendor	Operating System Platform	Deployment Agent	Detection Agent
Apple	MAC OS X	X	X
IBM	AIX 5.1	X	X
Microsoft	Windows Server 2003, Web Edition	X	X
Microsoft	Windows Server 2003, Standard Edition	X	X
Microsoft	Windows Server 2003, Enterprise Edition	X	X
Microsoft	Windows Server 2003, Datacenter Edition	X	X
Microsoft	Windows XP Professional	X	X
Microsoft	Windows XP Home (Personal)	X	X
Microsoft	Windows 2000 Datacenter Server	X	X
Microsoft	Windows 2000 Advanced Server	X	X
Microsoft	Windows 2000 Server	X	X
Microsoft	Windows 2000 Professional	X	X
Microsoft	Windows NT Server 4.0, Datacenter Edition	X	X
Microsoft	Windows NT Server 4.0, Terminal Server Edition	X	X
Microsoft	Windows NT Server 4.0, Enterprise Edition	X	X
Microsoft	Windows NT Server 4.0	X	X
Microsoft	Windows NT Workstation 4.0	X	X
Microsoft	Windows ME	X	X
Microsoft	Windows 98 SE	X	X
Microsoft	Windows 98	X	X
Microsoft	Windows 95 OSR2.5	X	X
Microsoft	Windows 95 OSR2	X	X
Microsoft	Windows 95	X	X
Novell	NetWare 4.11	X	X
Novell	NetWare 4.2	X	X
Novell	Netware 5.0	X	X
Novell	NetWare 5.1	X	X
Novell	NetWare 6.0	X	X
Red Hat	Red Hat Linux 6.2	X	X
Red Hat	Red Hat Linux 7.0	X	X
Red Hat	Red Hat Linux 7.1	X	X
Red Hat	Red Hat Linux 7.2	X	X
Red Hat	Red Hat Linux 7.3	X	X
Red Hat	Red Hat Linux 8.0	X	X
Red Hat	Red Hat Linux 9.0	X	X
Sun	Solaris 2.6	X	X
Sun	Solaris 7	X	X
Sun	Solaris 8	X	X
Sun	Solaris 9	X	X

1.2 Key features:

- **Patch Fingerprinting™:** PatchLink Update detection service will scan the system and determine which updates are applicable to a particular computer. Both the patch signature and fingerprints make a detection report, which is viewable in the report matrix. The PatchLink Master Archives currently host one of the largest automated patch fingerprinting repositories in the world.
- **Workstation Inventory (discovery agent):** PatchLink Update has an inventory discovery agent so it can pinpoint the needed software and hardware drivers for your client computers. The discovery agent also scans the client computer for the necessary signatures and fingerprints.
- **Built-in Security:** Uses digital security identification to register against the PatchLink Update Server. Before installing a downloaded update, it verifies the digital certificate, CRC check, compression and encryption on each file.
- **Role-based Administration:** (deemed a critical feature by government agencies as well as corporate customers) gives system administrators the ease and flexibility of distributing patch management ownership across a variety of systems, networks and physical locations.
- **Graphical Reporting** facilitates the IT administrator's ability to justify patch compliance; additionally, the reporting feature acts as an effective method for debriefing management on an organization's current patch status and/or network vulnerability.
- **Windows 2003 Server Compatibility** ensures widespread adoption and ease of use in most corporate and government environments.
- **Versatile Patch Compliancy Functionality** that allows system administrators to assess patch status by groups of computers, application, or severity.
- **Scalability** supports new server tuning parameters to allow very large numbers of agents per server.
- **Policy-based Patch Management** allows system administrators to enforce security settings and minimum patch baselines according to corporate standards.
- **Patch signature:** A technology that can scan the system and determine if the prerequisite for each patch has been met. This is done by checking the proper software version and proper hardware drivers.
- **Background downloads:** PatchLink Update uses a Secure Background Transfer Service (SBTS), which has built-in bandwidth throttling. The network administrator can decide how the bandwidth should be utilized during large deployments.
- **Chained installation:** The administrator can minimize repetitive rebooting by taking advantage of the Qchain.exe. If multiple updates are installed which require multiple reboots, the administrator, using Qchain, can deploy them with only one reboot. This minimizes the reboot process to increase the uptime for mission-critical computers. Qchain rearranges the DLLs in the proper order so the latest update will take effect. Administrators can choose this option during the deployment.
- **PatchLink Distribution Point:** PatchLink Update supports distribution point to facilitate patch caching and reduce valuable corporate WAN bandwidth utilization.

1.3 How it Works

Once installed onto your workstations, the Update Agents gather a list of software, hardware, services and patches installed on each computer within your network. The returned information can be viewed at any time in the Inventory section of the product, even if the workstation is disconnected from your network. With this detailed information, the PatchLink Update Server creates a complete analysis of your network profile that determines the patches, hot fixes, service packs and updates that are significant to your network. Based on this analysis, your subscription service will automatically download a series of Patch Reports.

The function of each Patch Report is to provide a detailed listing of the computers that require a specific patch as well as those that already have the patch. While viewing the report results, you have the option to schedule a patch rollout.

PLEASE NOTE: as recommended with all patches, you should first deploy the patch within your test environment before rolling it out into production.

Patch rollout is simple. Use the report to view the list of computers that do not have a particular patch update. Next, select the computers that should receive the patch and schedule the date and time for the rollout to occur. Once a rollout schedule has been created, a detail report shows you the status of the update – how many computers are downloading the patch, how many completed successfully as well as delivery error codes should there have been any failure conditions.

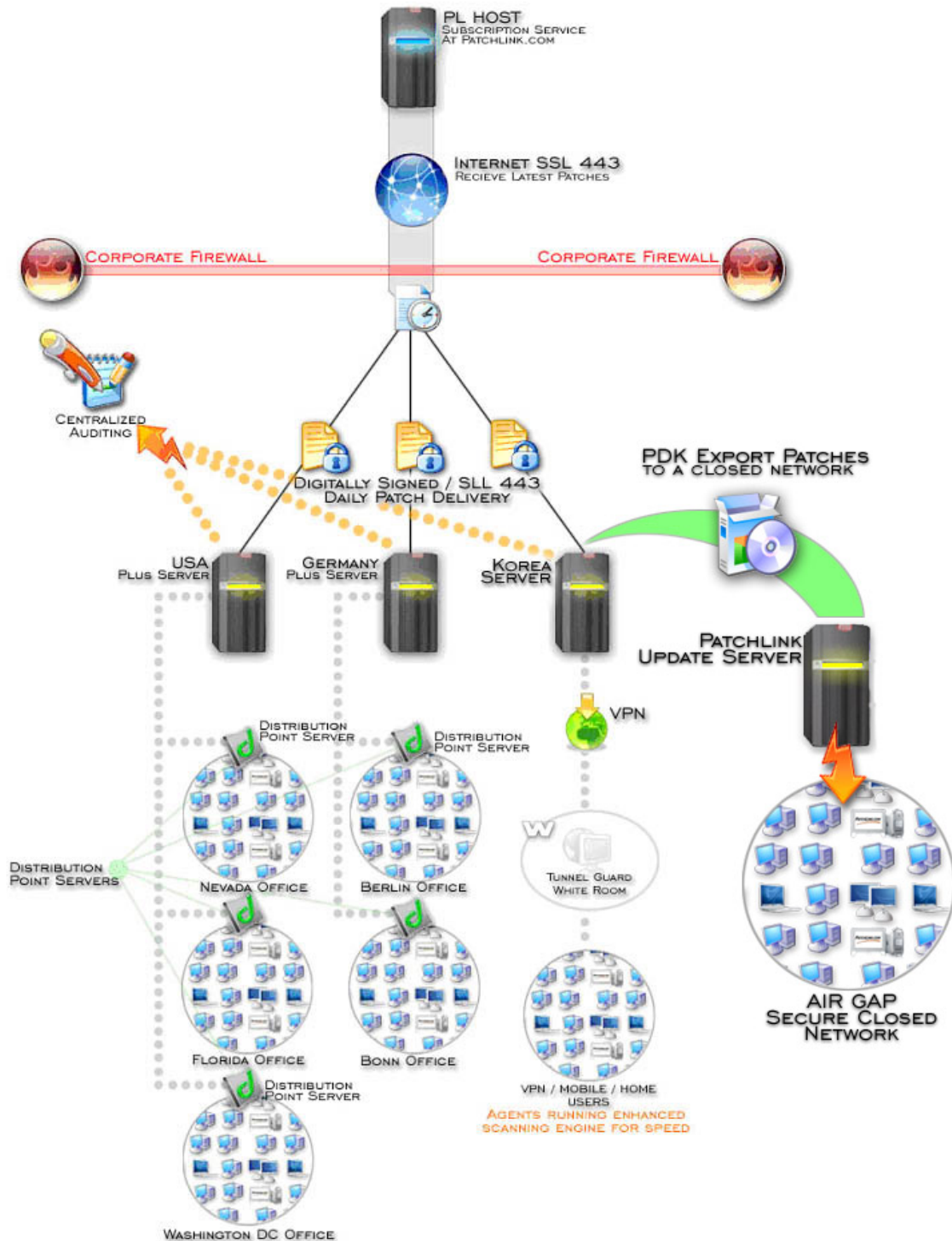
Once installed, your PatchLink Update Server will stay current with the latest patches and fixes by communicating with the PatchLink Master Archive server via its subscription connection. Anytime a newly released patch matches your stored network profile you will receive a proactive email notification. The next time you access the Update Server, a new report will show you the description and business impact of the patch as well as the list of computers that require it. At this time you can choose to rollout the patch or disregard it.

Unlike most other management software, the system is also virtually maintenance free: the Update Server is a completely self-sufficient unit that does not require backup or tedious database archival this is an adjective – probably not the right term to use here. For disaster recovery, merely reinstall the server using the same serial number and all of your installed Update Agent computers will automatically re-register.

As illustrated, the PatchLink Update Server has been designed to fit into your current administration should this be administration's or administrative job functions and proactively notify you as new patches and fixes become available. There are no new tools to install and learn; everything can be done using your web browser. Because it is so automated, this solution can also help to greatly reduce the window of opportunity for patch-related server and workstation vulnerabilities.

ENTERPRISE WIDE SOLUTION

INFRASTRUCTURE OVERVIEW



1.4 System Requirements

System Requirements for Evaluation Purposes:

To install the server software you will need a server, desktop or laptop computer model with 256 MB of RAM and at least 5 GB of free disk space. A 500 MHz or better CPU is recommended for minimal system operation.

The evaluation software can be loaded on Windows 2000 Professional as well as Windows 2000 and Windows 2003 Server and Advanced Server. It is recommended that the PatchLink Update software be evaluated in a small environment dedicated for testing software.

If you plan to test in an isolated environment, please build your server somewhere outside the test environment, allowing it to obtain its subscription and download all critical packages via its internet connection, then move it into your testing environment.

The PatchLink Update Server software comes with Microsoft SQL Server 2000 Desktop Engine (MSDE 2000). This version of SQL server is limited to 8 concurrent database connections and is NOT intended to be deployed in a production environment.

Windows 2000 Service Pack 4 is also required. Please install it from <http://www.microsoft.com/windows2000> before continuing on.

PLEASE NOTE: Do not under any circumstances attempt to install on a computer that has personal firewall products, popup killer, web server security tools, domain policy restrictions or any version of Microsoft SQL Server product installed on it. You may lock down your configuration AFTER installation of the software, if so desired.

1.5 Hardware Requirements

The hardware requirements for production environments vary depending upon the number of clients that are being updated by the PatchLink Update server.

- For an installation of up to 100 PatchLink Update Clients it is recommended that a dedicated server with minimum of a Pentium III class, 700 MHz+ CPU and 512MB+ of RAM with 5 GB of free disk space
- For an installation of over 100 PatchLink Update Clients it is recommended that a dedicated server with minimum of a Pentium IV class 1.4 GHz+ CPU and 1GB+ of RAM with 5 GB of free disk space
- An additional 1 GB of RAM is recommended for each additional 1000 Update Clients
- Additional disk space may be needed as the number of patch packages in the local cache increases. Allocating at least 20 GB of disk storage would allow for this growth.

1.6 Operating System Requirements for Production Environments

The operating system must be a clean install of Windows 2000 Server. For enterprise solutions requiring load-balancing and other advanced features, Windows 2000 Advanced Server should be installed. To save time with the server installation and increase the security of the server during installation, all the latest service packs, security updates and hot fixes should be installed immediately after installing the operating system.

The Internet Information Server (IIS) must be installed along with the operating system. Should you need to add Internet Information Server to your server, merely go to the Start Menu and click Settings > Control Panel, then run the Add/Remove Programs application and click on Add/Remove Windows Components. If Internet Information Services is not checked, check that option and press Next> to install it.

Your computer must also have a browser connection to the Internet. Without an Internet connection you will be unable to obtain your patch subscription and patch packages from www.patchlink.com and storage12.patchlink.com. If necessary, the Update Server can access the Internet through an un-authenticated proxy server, since the various replication tasks run as services on the machine when there is no user actually logged in. If you are currently using an authenticated proxy, we recommend that you perform your evaluation in a different environment (test lab, home PC, etc) to avoid having to configure additional proxy rules for your corporate Internet gateway. Be sure to allow access to both subscription servers through your firewall:

https://www.patchlink.com	206.124.169.50	Port 443
https://storage12.patchlink.com	216.205.112.66	Port 443

Once these steps are completed, make sure that you are logged into your computer as the local computer Administrator account, who **MUST** have rights to install software onto the local system, and then begin the installation process outlined in the next few pages.

PLEASE NOTE: Installation onto a Primary Domain Controller (PDC) is not supported in this release of software; however this is also not a recommended configuration for the system. Please install the product on a member server within your domain or Active Directory environment. The product also installs on any stand-alone workgroup server.

1.7 SQL Server Requirements for Production Environments

The PatchLink Update Server software comes with Microsoft SQL Server 2000 Desktop Engine (MSDE 2000). This version of SQL server is limited to 8 concurrent database connections and is NOT intended to be deployed in a production environment. To deploy the Update Server in a production environment you **MUST** upgrade the MSDE 2000 SQL Server to a fully licensed SQL Server 2000.

The licensing of the SQL Server 2000 product can be confusing especially since there are three ways to license the product. Here are the three licensing options:

- **Processor license.** Requires a single license for each CPU in the operating system instance running SQL Server. This license does not require any device or user client access licenses (CALs).
- **Server plus device CALs.** Requires a license for the computer running the Microsoft server product, as well as a CAL for each client device.
- **Server plus user CALs.** Requires a license for the computer running the Microsoft server product, as well as a CAL for each user.

Since the PatchLink Update Server interface to the SQL Server database only appears to the SQL Server as one client device and one user through the use of the Internet Server Application Programming Interface (ISAPI) interface, the only SQL Server 2000 license ever needed is the processor license.

1.8 Upgrading to version 6 of Patchlink

There are prerequisites to upgrade to version 6 of patchlink:

Open your web interface to Options / Support – Check the version you are currently using in the:

- Patchlink Update server information panel
- PatchLink Update Server Version:

The version must be 5.00.01.61 or higher to upgrade directly to Version 6.x

- If you are on version 5.00.01.47 or lower install: step 1, step 2 then step 3
- If you are on 5.00.01.54 install: step 2 then step 3
- If you are on 5.00.01.61 or higher install: step 3

Step 1: install the current hot fix

Download from <https://storage12.patchlink.com/downloads/>

1. Download and extract to c:\winnt\temp.
2. From Dos, type: net stop W3SVC /Y.
3. From Dos, type: net stop IISADMIN
4. Go to c:\winnt\temp\HOTFIX5.0.1.54 Folder and run hotfix.exe /v
5. The Hotfix.exe will automatically restart the Windows 2000 Computer.

After you install this hot fix check the update server log found in the directory which you ran the hot fix from. Make sure there are no errors in this log before going to the next step

Step 2: Install the 5.00.01.54 to 5.00.01.61 incremental update (you must be on version 5.00.01.54 to install this hot fix)

<http://storage12.patchlink.com/downloads/50161.zip>

1. Download and extract to c:\winnt\temp.
2. From Dos, type: net stop W3SVC /Y.
3. From Dos, type: net stop IISADMIN
4. From Dos, cd to c:\winnt\temp\QA PLUS PATCH 5.0.1.54 to 61 12-05-2003 Folder and run the hotfix.exe/V to display the GUI for the status of the Hot fix.
5. The Hotfix.exe will automatically restart the Windows 2000/2003 Computer.

After you install this hot fix check the update server log found in the directory which you ran the hot fix from. Make sure there are no errors in this log before going to the next step

Step 3: install the 5.00.01.61 or higher to 6.00.45 hot fix (this will also upgrade lower version of 6 to this new version)

To download the Hot fix Update to upgrade to 6.00.00.45:

<https://storage12.patchlink.com/securedownloads/PLUS6.0.0.45Hotfix.zip>

Username: v6release
Password: ikyy5cw4

1. Download and extract to c:\winnt\temp or c:\windows\temp.
2. Open a dos shell and CD to the c:\winnt\temp or c:\windows\temp directory.
3. Type "net stop iisadmin /y" to stop the IIS Admin Services
4. CD to the folder PLUS PATCH 5.01.61 to 6.0.0.45
5. Run Hotfix.exe /V to install the Server Hot fix.
6. Please note that the Server Hot fix will restart the PatchLink Update Server.

After you install this hot fix check the update server log found in the directory which you ran the hot fix from. Make sure there are no errors in this log

Clean install of Version 6

To download the complete installable build of 6.00.00.45:

PLUS6.0.0.44.exe is a complete installation of the new build, if you plan to install this version on to a fresh Windows2000 or Windows2003 server.

If you've already got a PatchLink Update Server installed with version 6, please use the PLUS6.0.0.45HOTFIX.zip file. Just extract the zipfile and run the hot fix EXE that it contains in order to upgrade your existing update server to the latest version. Note that early access customers should be running the hot fix only if they have Version 6.0 already installed and running on a server.

<https://storage12.patchlink.com/securedownloads/PLUS6.0.0.45.exe>

Username: v6release

Password: ikyy5cw4

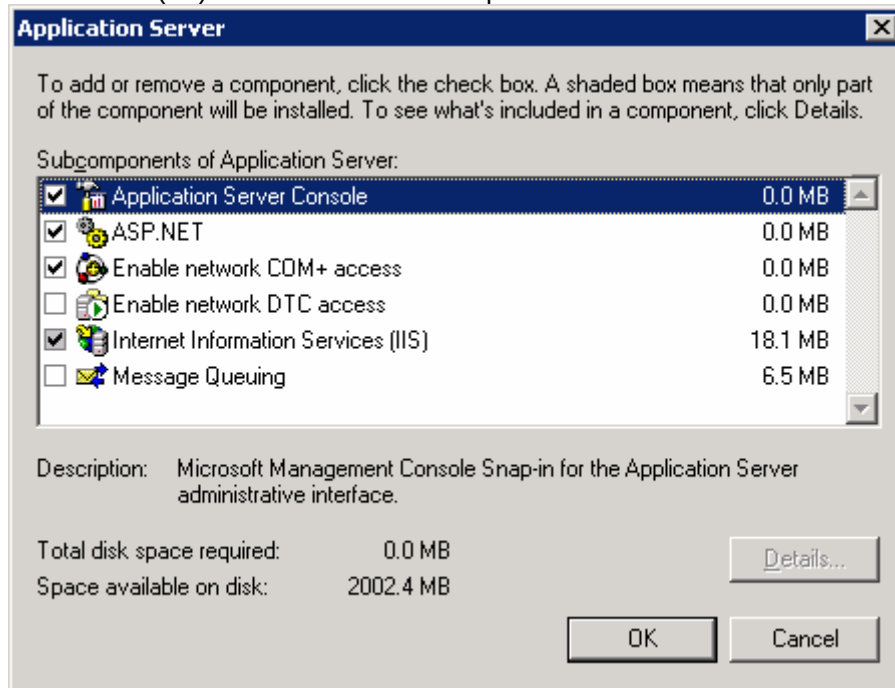
1.9 Typical Installation

A typical installation of 10,000 or fewer Agents consists of a single Patchlink Server that gathers Vulnerability Fixes from the Internet where they can be viewed by the Web console and distributed to the Agents thru the distribution point servers, which pass the data on to locally connected agents. Each Agent inspects its local computer and reports any relevant vulnerability back to the Patchlink server. The Web console oversees this activity. It connects to the Patchlink server and periodically updates its display to reflect changes or new knowledge about your network. When vulnerabilities are discovered, the admin can then target patches or other fixes to the appropriate computers. The progress of the fixes can be followed in near real-time as they spread to all the relevant computers and, one by one, eliminate their vulnerabilities.

1.10 Installation on fresh Windows 2003 Server

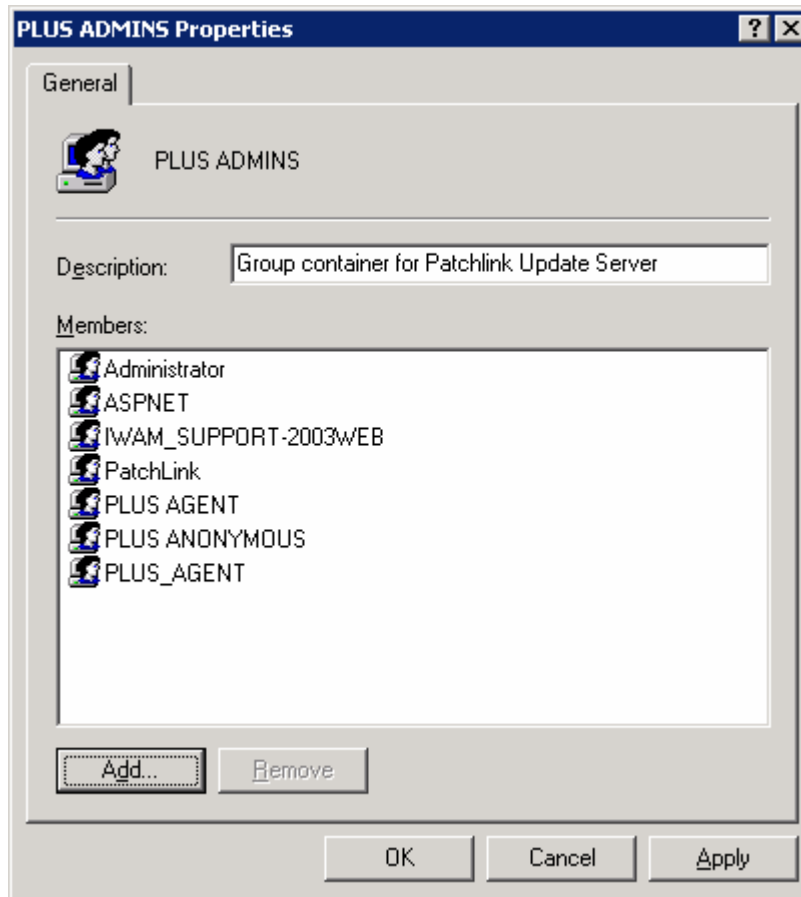
Should you wish to install the PatchLink Update Server to Windows 2003 Server, install a fresh copy of the operating system without performing any additional policy, port or service lockdowns before installing the PatchLink Update product. Also please note that you must NOT install the product from a Remote Desktop session in this release - please install from the server computer itself.

- 1) On your Windows 2003 Server, please go to add/remove programs => Add/Remove Windows Components => Application Server => Details => Verify that Internet Information Services (IIS) and ASP.NET Subcomponents are selected.

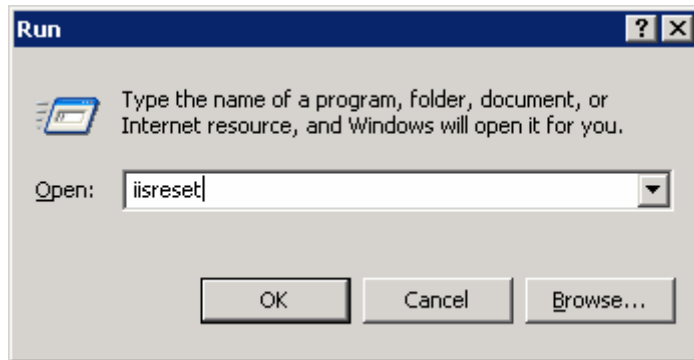


- 2) Follow the installation instructions in section 2.1 of this document to install the PatchLink Update Server software on a Windows 2003 Server.

- 3) Once the Windows 2003 Server is restarted, please log on locally and right mouse click on My Computer => Manage => Groups => Make the ASPNET and IWAM_COMPUTERNAME local account members of the PLUS ADMINS Group. Click OK to save your settings.



- 4) Once the two local accounts have been added to the PLUS ADMINS Group, open run prompt and type "iisreset" and "OK" button to restart the Web Server so the changes can take affect.



1.11 Migration to Windows 2003 Server

Because Windows 2003 Server includes many new security enhancements and a much more robust version of Internet Information Server, we do not recommend upgrading an existing Update Server from Windows 2000 to Windows 2003 server. Should you wish to run PatchLink Update Server on Windows2003 Server, please be sure to install the PLUS on a clean OS rather than performing an upgrade install. This will ensure that your PLUS website is correctly configured with the necessary settings to allow our product to operate in the W2K3 environment.

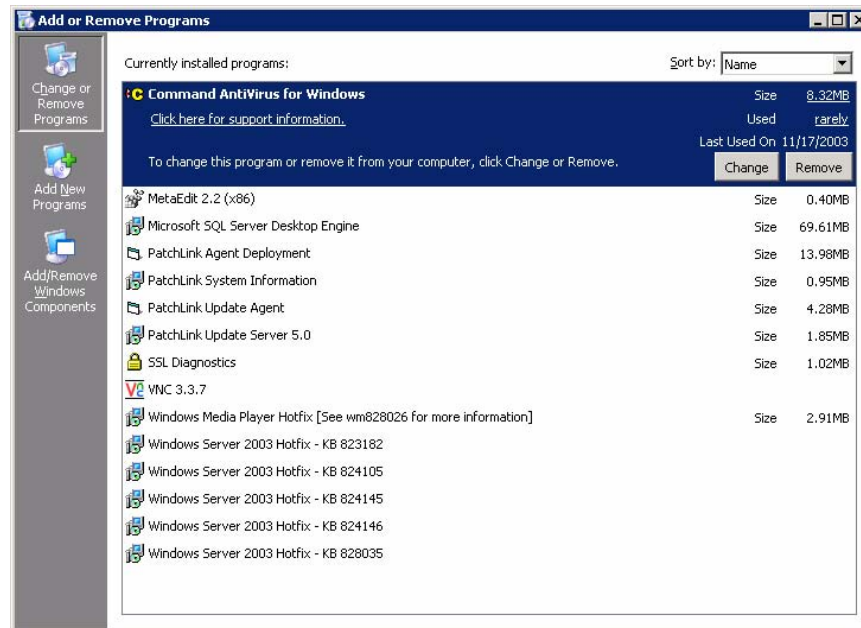
1.12 Windows 2003 Server Support

PLUS now supports the use of Windows 2003 Server and 2003 Server Web Edition. Windows 2003 Server Web Edition however must only be used in small PLUS deployments of 300 nodes or less. This is due to the inability to upgrade the Microsoft MSDE database to a full Microsoft SQL Server license.

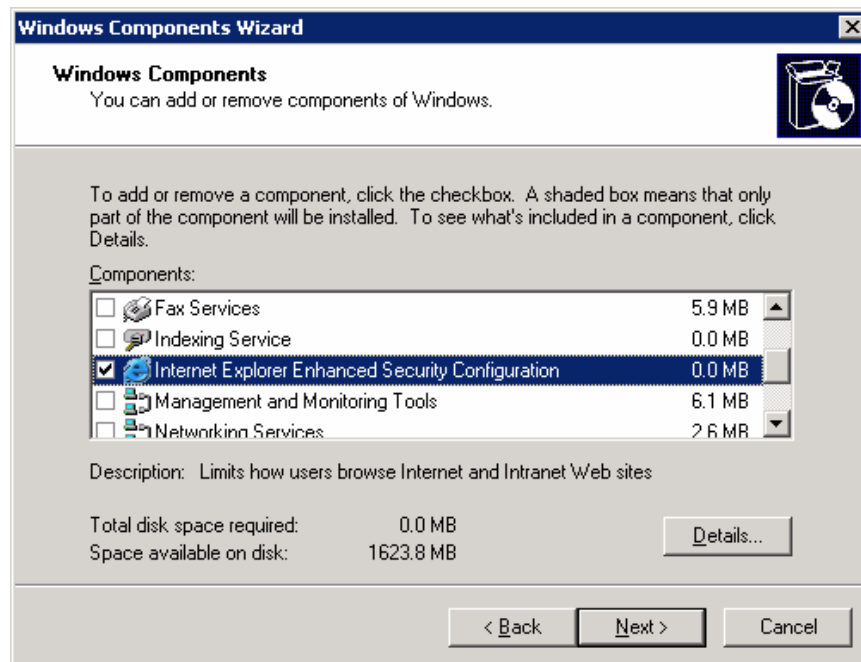
The steps outlined below will configure your Windows 2003 server for PatchLink Update Server (PLUS). These steps should be performed before installing PLUS and are necessary to ensure a successful install.

Configuration Steps

- 1) To configure Windows 2003 Server for use with PLUS first select Start/Control Panel.
- 2) Then select **Add/Remove Programs**

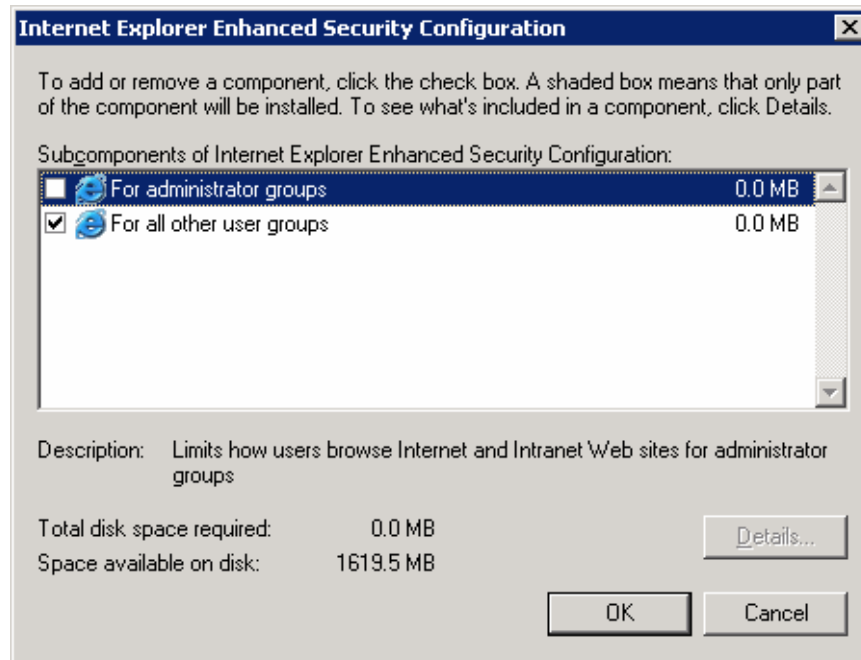


- 3) Then select **Add/Remove Windows Components**

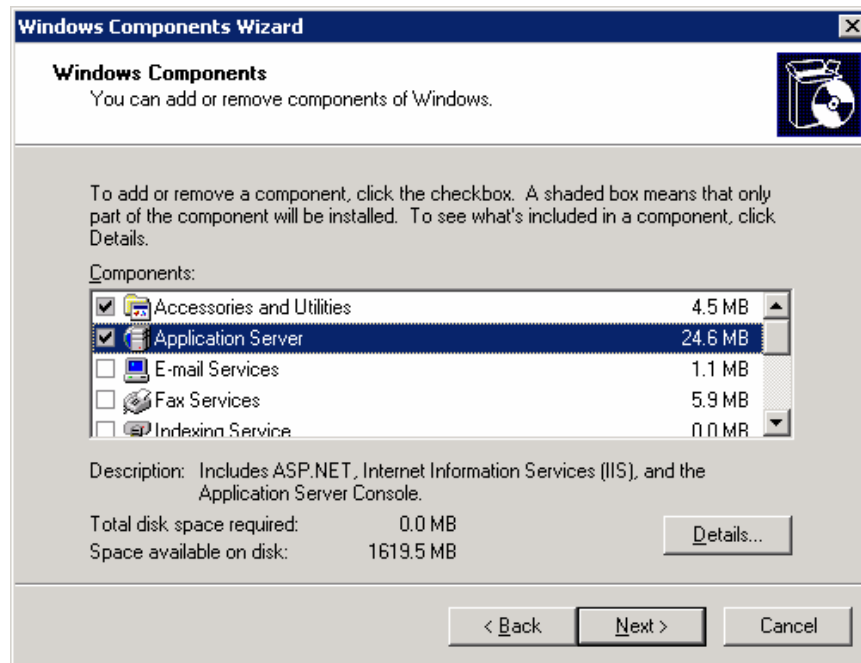


NOTE: The next step is only necessary if you require the ability to administer the PLUS from the server console. It is not recommended that you perform this step unless it is absolutely necessary. Administration of the PLUS is typically performed from a workstation via a Web browser.

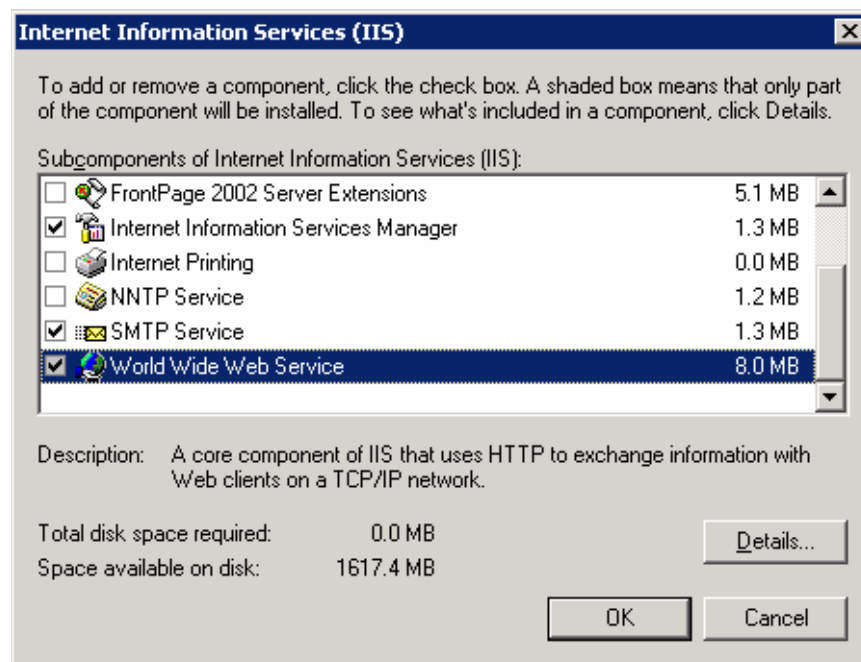
- 4) If you need to administer PLUS from the console, select Internet Explorer Enhanced Security Configuration and click details. On this screen, uncheck the “For Administrator Groups” option and click on OK.



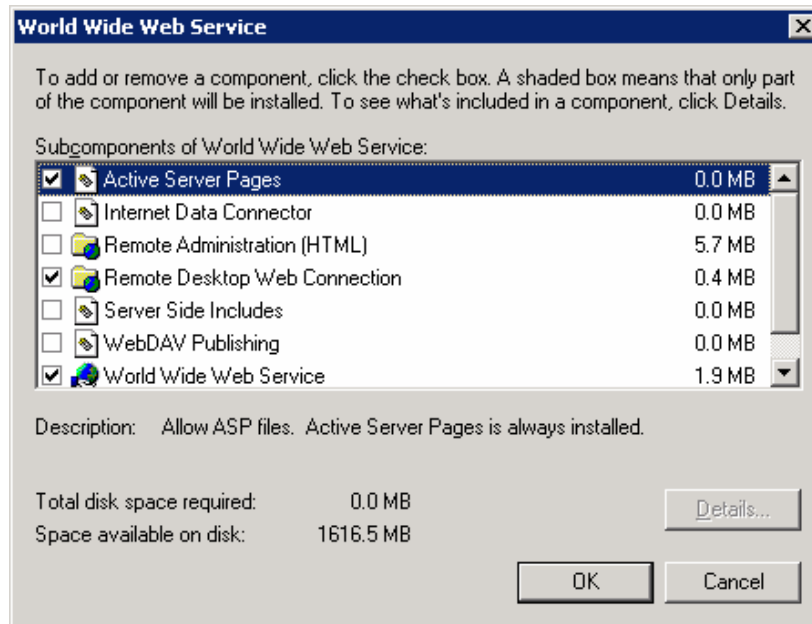
- 5) The next step is to go back to the Add/Remove Windows Components screen and check the box next to the Application Server component and then click the Details button.



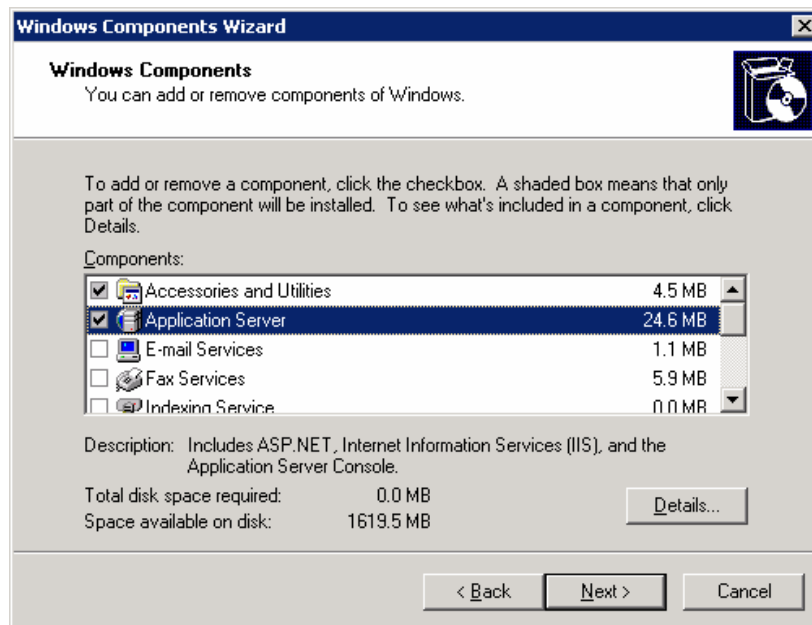
- 6) Check the box next to the ASP.NET component and then select the Internet Information Services component and click Details. Select the World Wide Web Service component and click Details.



- 7) Check the box next to Active Server Pages and click OK, OK, OK.



- 8) Click Next> and insert your Windows 2003 Server CD if prompted.



9) Click Finish



This completes the configuration for Windows 2003.

2. What's new with PatchLink Update version 6.0?

PatchLink Update 6.0 brings an already superior patch and configuration management product to a level unsurpassed by any other solution on the market today. Many improvements and features have been added made to make PatchLink Update easier to use and in the world of patch management, easier is better! The new Agent Management Center makes deploying the computer agents seamless and versatile with complete integration with Microsoft's Active Directory and LDAP directory services.

Several improvements have been made to better inform the administrator as to the status of deployments. There is also a great deal more flexibility as far as the creation of administrative computer groups is concerned. Here is a list of the major changes made in PatchLink Update to make the job of patch and configuration management more versatile and easy.

2.1 Agent Management Center (See Section 3.6 for more details)

- Enterprise Computer Discovery
The Agent Management Center allows the patch administrator to automatically discover computers within a specified IP address range, NT or Active Directory domain, LDAP Organizational Unit. The results of the discovery will tell the user whether the computer has the agent installed or not and allow installation on computers that do not have a PatchLink agent running.

2.2 Application Programming Interface

- A new Application Programming Interface (API) to allow the user to query the SQL database. This will provide the user with the ability to check what the status of any computer is at any particular moment.

2.3 Improved Patch Deployment

- Chainable Deployments
Chainable deployments allow the administrator to define a group of packages to be deployed to a group of computers (many-to-many) without the need to reboot the computers after each deployment. This cuts down on the number of reboots that need to be performed, thus increasing computer availability.

2.4 Better User Information

- Better Search Features
The **Vulnerabilities** page and all the other top level pages have increased searching functionality. For instance, on the **Vulnerabilities** page, you can now search via vulnerability name/CVE number, status, impact, and the original group search.
- Status Page
The PLUS **Status** page gives users a set of comprehensive indicators on what PLUS is currently doing or scheduled to do. This includes all deployments in the queue for any given period of time, status of the Discover Applicable Updates process (DAU) and a better indication as to the status of the PLUS subscription replication between PLHOST and the PLUS server.

- Status Window

PLUS now provides detailed agent deployment status logging allowing each sub-transaction to be logged and displayed back on the PLUS.

2.5 Smarter Agents

- Smarter Client Agent

The client agent now triggers the PLUS to reschedule the DAU process for that particular computer anytime an end user installs any hardware or software thus giving an immediate update to PLUS as to the vulnerabilities of the computer.

- Smarter Discovery Agent

A new agent policy setting allows the user to run the DAU at variable speeds enabling better control of network bandwidth utilization.

2.6 Windows 2003 Server Support

True Windows 2003 Server support is provided for Web, Standard and Enterprise versions.

Note: Windows 2003 Web version supports a limited number of agents due to MSDE limitations.

3. Getting Started

3.1 Using This Guide

Use this guide as a reference to describe PLUS as in what it is, what it does, and how to do it. It is best to follow this guide sequentially as you begin using PLUS, as certain sections pertain to and reference others that are documented later in the manual.

Most screenshots contained in this guide were taken using Windows XP operating system set with the default (blue) color scheme. The color schemes, buttons, and other items may vary slightly on your operating environment depending on what operating system you are running and your selected theme.

3.2 Understanding the Interface

Contained in each section of PLUS, as illustrated by this document, are certain page functions and features designed either to aid the user's tasks, or to simply enhance other functions. Certain pages contain specific functions and features and these various functions and features may or may not be present depending on what page you are on. Note the **Page Functions** heading in each section to view which features are present. The standard page functions and features are broken down as follows:

- Help

The PatchLink Update Server (PLUS) is a very comprehensive, web-based interface, designed to provide PatchLink Users the information for what they need in a timely manner to properly patch and manage your network. It assists new users in learning the product, yet keeping all of the core functionality available for advanced users. Throughout PLUS, context sensitive help is provided by clicking on the **Help** located in the top menu or the  icon found on the top of every wizard and property page. Many of the user interfaces have fields that contain additional information that is displayed when your mouse moves over one of those fields.

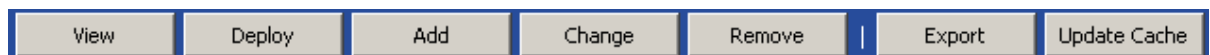
- Navigation Menu



A horizontal navigation bar with a blue background and white text. The items are: Home (highlighted in orange), Vulnerabilities, Inventory, Packages, Computers, Groups, Users, Reports, Options, and Help.

The user interface provides a consistent and easy to use navigation menu, which is always present across the top portion of the screen. This navigation menu quickly takes you to the various major sections of PLUS, as well as providing secondary notification of what section you are currently in. This navigation menu will behave differently based on your defined access rights associated with your user role. A section's name will not highlight or take you to the section if you do not have access to that section.

- Action Menu



A variety of context sensitive actions are always located along the bottom of the page. These buttons provide quick access to all the common actions available for each page.

Like the navigation menu, the action menu functionality also depends on your user role (and its defined access rights) and the view you are working in (if a filter dropdown selection is applicable). If you do not have access to a button, the button will be grayed out and non-functional. Note the **Action Menu** heading in each section to view which actions are present.

- Display and Hide

The display more information (+) and hide (-) information functions appear regularly throughout PLUS. If the display and hide function is present on a certain page, it will be identified each section's **Page Functions**. Click on the + to display additional information and statistics about the represented item. Click the - to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (-, +) is only available for Microsoft Internet Explorer at this time.

- Advanced Page Search, Filtering, and View Saving

Starting with version 6.0, the filtering capability of PLUS has been greatly enhanced. Now you can search, filter, and save results views as your default view for the next time you visit the page. This makes the job of finding what you are looking for much easier and less time consuming.

The advanced page search, filtering dropdown menus, and saving functions appear in various PLUS pages.



Depending on what page you are viewing determines your ability to search, filter, and save your viewable results.

For instance, you may search **Inventory** for more granular results by entering the computer name text into the **Search** field and clicking on the **Update View** button. This will return the computer(s) having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Page search, filtering dropdown menus, and saving functionality varies depending on what page you are on. To understand the full advanced page search, filtering dropdown menus, and saving functions appearing on the PLUS pages, see the respective **Page Functions** sections of this document where applicable.

- Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

- Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

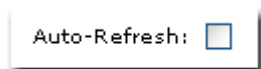
- Display (Pagination)

Depending on the amount of items available for display and what page you are viewing, determines the display function. The Display function, if enabled, is located at the bottom above the Action Menu.



- Next: To display the next page of computers, click on the next button. If the last computer is displayed, the next button is disabled.
- Previous: To display the previous page of computers, click on the previous button. If the first computer is being displayed, the previous button is disabled.
- Computers per Page: The computer list initially displays up to 100 computers per page. To change the number of computers to display per page, enter a new number in to the Computers per Page input field. To display all computers enter a zero in the input field.

- Auto Refresh



Where present and when selected, the Auto Refresh function automatically refreshes the page every 15 seconds.

- Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the PLUS and are **not** visible in Netscape.

3.3 Defining Access

Determining who gets access to PLUS, what they can see, and what they can do is completely user-configurable. The goal of PLUS Security is not to mandate how you define your security policies, but only to allow you the ability to institute your security policies effectively for PLUS. Security access is determined by two mechanisms: Windows-based authentication and PLUS access rights.

- Windows-based Authentication

Authenticating to PLUS is handled by the Windows operating system. Any user(s) who are members of a local Windows group, PLUS Administrators, will gain all the necessary rights and abilities to log on to the web site. Authorization of what users can and can not do is handled by Access Rights (see below). Upon installation, the PatchLink user (who is created during the installation) is given the Administrator user role, but you may remove this at any time, as long as there exists at least one user who belongs to the Administrator user role.

- PLUS Access Rights

Once a user has authenticated into PLUS, their assigned user role is checked to see what features (sections of PLUS) and functionality (actions they can perform in those sections) they have. Each user role is assigned its own set of groups and computers (computers outside of the membership of the assigned groups) on which their access right-based functionality operates.

If a user manages to get past the Windows security (Domain User who is not a member of the local PLUS Administrators group for example), they will be unable to view any sections of PLUS, see any groups or computers or perform any actions on them. If a user does not have access to a given section, they will be given an access denied error message.

In the Users Section, the Roles tab is where these roles are defined, while the Users tab is where you can add or remove users to PLUS and assign them a user role.

3.4 Agent Behavior – Defining Your Policies

Before getting into the installation of agents on to the client computers of your network, the behavior of how those agents will act needs to be defined. At installation, the only single mechanism that defines this is found in the **Options** section, under the **Defaults** page.

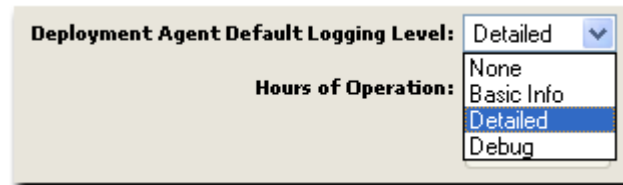
Since all of the groups are installed using the **Empty Agent Policy Set**, this is the single place that will affect your agent's behavior.



There are only four individual items that make up an agent's behavior and they are all easily configurable from this page. Of the four items, three can be overridden by a group's **Agent Policy Set**.

- **Logging Level**

Determines how much data you want your agents to save to their log files. The four options are:



- **None:** only errors are logged.
- **Basic Info:** errors and the very basic information is saved. Example: when it is performing a deployment it will indicate that it had a deployment to do.
- **Detailed:** errors and more explanation of what the agent is doing is saved. Example: deployments, including what they deployments are, and when agent policies are changed, including what they are, are logged.
- **Debug:** log everything and every step the agent does. This should only be used when you are validating the agent's behavior or its actions. This mode will generate megabytes worth of data on a busy system.

Note: The agent log files are deleted every time the Refresh Inventory Data System Task is deployed to an agent.

- **Communication Interval**
Determines how much time the agent will sleep between communication with PLUS. When it communicates with PLUS it is checking to see if it has any policy updates or if it has any deployments to do. This interval is critical to PLUS; if the interval is too high, the agents will not get their tasks in a reasonable amount of time. If the interval is too low, PLUS (and your network traffic) will constantly be busy and other agents will not be able to get their tasks. Interval rates typically vary between 15 and 60 minutes depending upon number of nodes, network architecture and bandwidth.
- **Hours of Operation**
When enabled, this value determines when the agents shall start and stop communicating with PLUS. If the agent is in the middle of a deployment and the agent's hours of operation expire (exceeds the designated stop time) it will finish what it is currently working on and continue the rest of the deployment at the next Hours of Operation interval.
- **Concurrent Deployment Limit**
This value determines how many deployments can be given to the agents at any given time (if a deployment is scheduled for more than an hour for a particular agent, that deployment is no longer counted). This is a safeguard that will reduce the chance of any of your PLUS' systems from being overloaded. This is the only value that cannot be overridden by a group's **Agent Policy Set** as it limits deployments for all agents.

3.5 Agents and Installing Them

Both the deployment (also known as **Deployment Agent**) and **Detection Agent** are bundled together and installed at the same time. The deployment agent is a service that is constantly running to ensure that when deployments are ready to start, policy changes, etc., the agent will act on them in a timely manner. The behavior of this agent is entirely defined by the agent's policies, whether the agent is using the default agent policies for PLUS or the superset of the group's agent policy sets the agent is a member of. The detection agent will run only when the user on the individual computer initiates it, or the deployment agent deploys the **Discover Applicable Updates System Task**.

Installing agents is a simple function and there are various installers available to install agents on to your computers. They can be found by clicking on the **Install** button in the **Computers** section. This will initialize a screen showing the available PatchLink Update Agent Installers.

Note: If you cannot access the Computers section or do not have access for the Install button speak with your PLUS Administrator on obtaining access to those sections of the product.

The **Agent Installers** page displays the various installers you can use to register computers to PLUS. For each agent installer, there is useful information you should read first to determine which one to use for which computers. Each agent installer is different from the operating systems it works under in pertinence to its requirements or behavior.

Read each section carefully to determine the best options for your needs. If one does not work for a particular computer, check the others or access the PLUS Forums to see if there is a better option available for you. Without the agents installed on your computers, you will not be able to determine what is patched and what is not patched, nor will you be able to deploy any patches.

The various agent installers are:

- Single Agent Installer for Windows (Win95 to Win2k3)
- Single Agent Windows MSI Installer (Win95 to Win2k3)
- Silent Agent Installer for Windows (Win95 to Win2k3)
- Domain-wide Agent Deployment Wizard for Windows (Win2k to Win2k3).
Available computers are captured from the Primary Domain Controller.
- Single Agent Installer for UNIX (Solaris, Red Hat Linux)
- Single Agent Installer for NetWare (4.11 to 6)
- PatchLink Distribution Point

Once a computer has registered its agent against PLUS, the PLUS Administrator can assign it to various user roles so others can access or view it.

- See Section 10.4 for more detail on the PatchLink Distribution Point.

3.6 Agent Management Center (AMC)

The PatchLink PLUS features a new enterprise-wide agent distribution mechanism called the Agent Management Center. Through the use of Deployment (Client) Agents, Package Editor, and the Agent Management Center, you can securely send software, documentation, scripts (SW, HW and Services) or any other content across your network, from small Intranets to huge Extranets, or even the Internet itself.

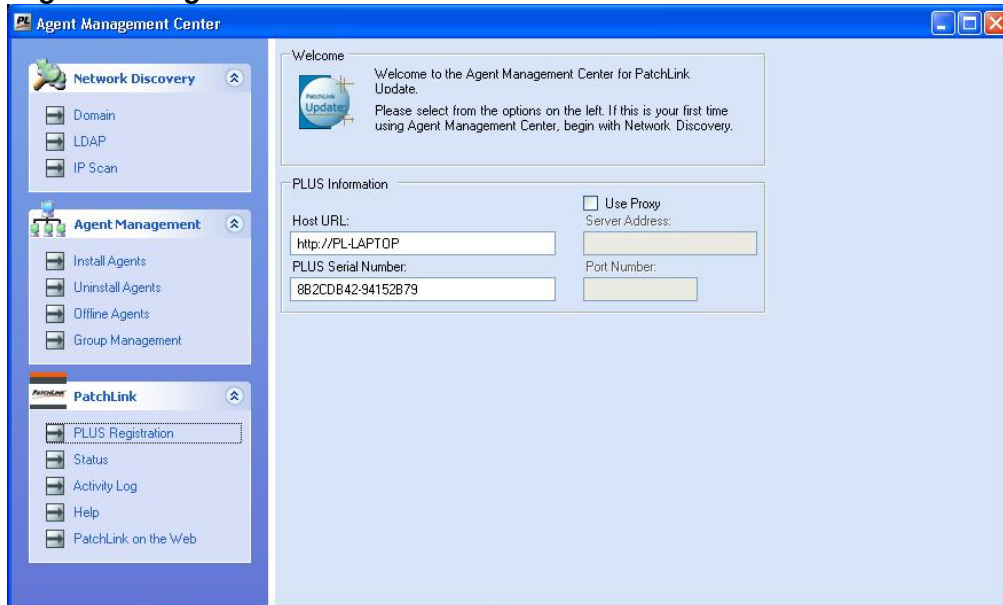
The major features of the **AMC** allow you to perform network host discovery, install / uninstall PLUS agents, and agent management functions including adding agents to groups or user roles, and removing agents from PLUS if they have been offline for an extended period.

AMC is not intended for use (and doesn't work) on Windows 98/ME OS.

AMC installation to XP machines requires that the XP computer is a member of a domain.

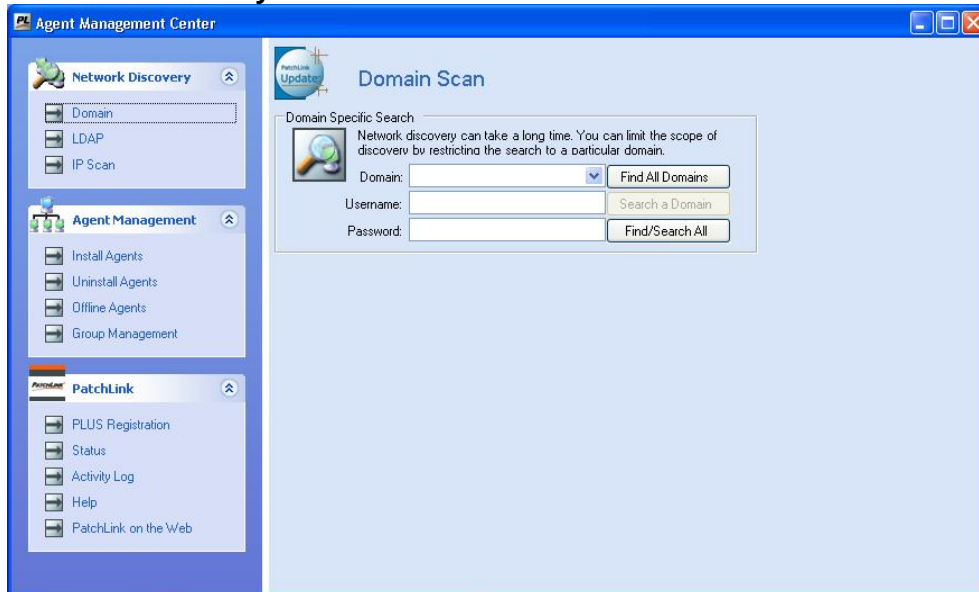
- Enterprise Computer Discovery
The Agent Management Center allows the patch administrator to automatically discover computers within a specified IP address range, a Windows domain or an LDAP Organizational Unit. The results of the discovery will tell the user whether the computer has the agent installed or not and allow installation on computers that do not have a PatchLink agent running.
- Agent Installation
The AMC makes the task of agent installation easier by allowing users to selectively install the agent on a few or many computers that they choose at one time.

Agent Management Center Main Screen



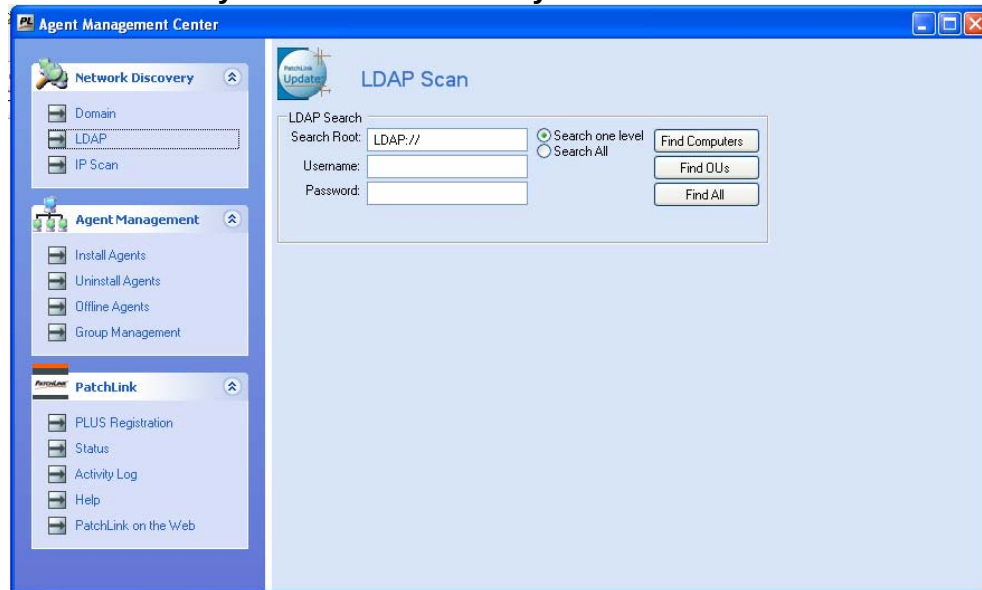
The Main Screen is the screen first displayed when deploying the AMC from the Windows/Programs menu. From this page you can choose to perform a network discovery, perform agent installation and management functions or access the PLUS product registration page and other PLUS functions. Information needed by the agents for use in the installation process is entered here. The Host URL for the PLUS server and its PLUS Serial Number should be entered here before you deploy agents.

Network Discovery Screen



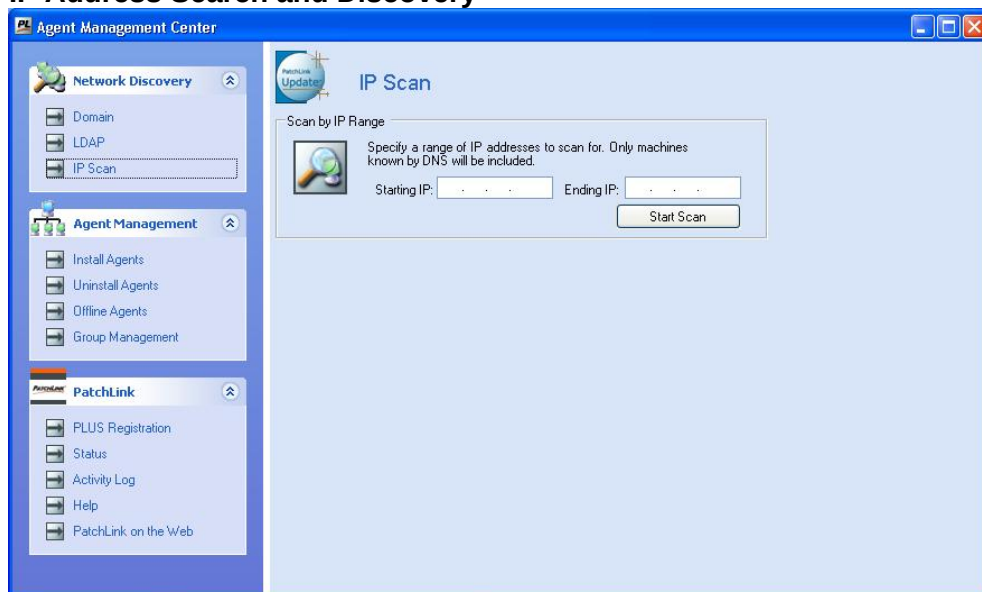
The **Domain Discovery** screen allows you to perform a **Domain Specific Search** or a **Search All Domains** to discover all the computers in the domain. You simply enter the name of the domain in the Domain field or select the Find Domains pushbutton to find all the domains in your network.

Active Directory Search and Discovery



The Active Directory/LDAP Search and Discovery screen allows the user to search for computers within the directory tree from the root directory. The username and password for the Active Directory Administrator account can be entered in the corresponding fields but may not be necessary depending on your LDAP setup. All that is really needed is that your user permissions include read permission on the LDAP directory. From here you can select whether you want to only search one level or search all levels of the LDAP root. You can also choose to find computers, LDAP Organizational Units or find all the elements in the directory.

IP Address Search and Discovery

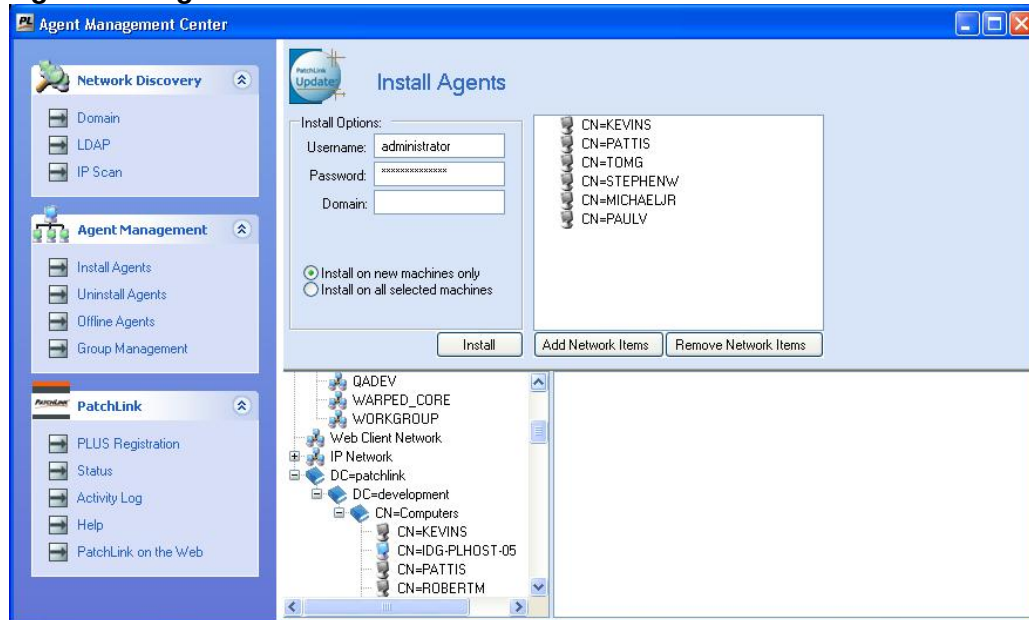


The IP Scan Screen allows the user to search the network for computers by their IP addresses. The IP addresses must be registered within the Domain Name Service (DNS) of the DNS domain in order to obtain the computer name.

Enter the starting and ending IP addresses that you want to scan for and select the Start Scan pushbutton to begin your scan. Multiple ranges of IP address can be searched simultaneously.

Note: System Discovery using IP Scan will likely set off Intrusion Detection systems. Please be advised of this before you use this method in your environment and notify the appropriate security personal.

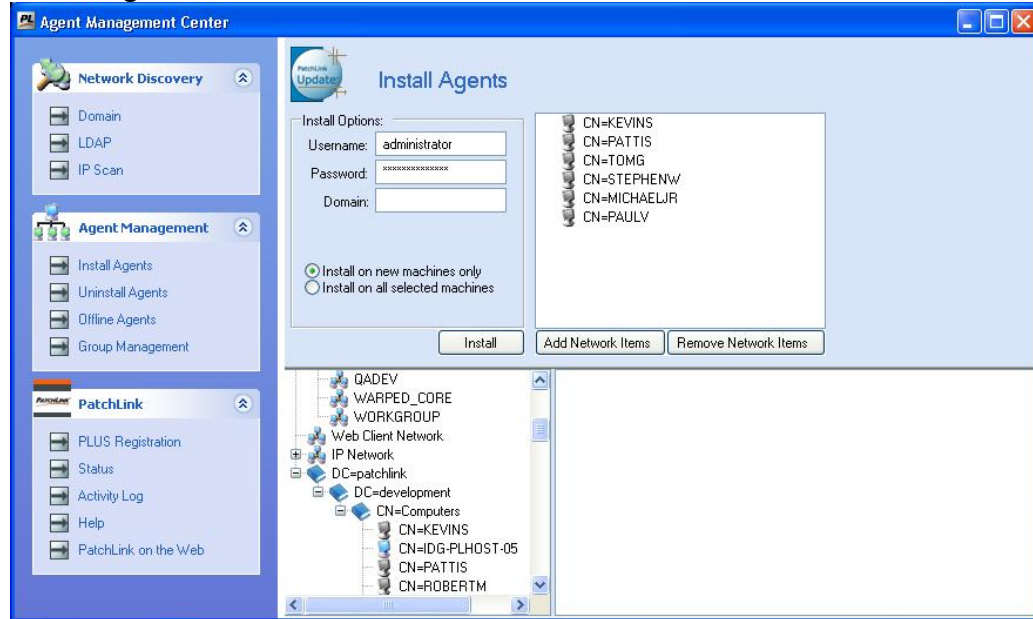
Agent Management Screen



The Install Agents screen is the place where you perform the agent install after you have discovered the computers on your network. The user entered in the Username field must have Administrator permissions in order to install the Update Agent. You can choose whether you want to install on new computers only or reinstall on a previously discovered computer. You must also choose which install method for AMC to use. The recommended method of installation is using the WMI Install option but can only be used if the WMI service is running on the computer. If the WMI service is not running then you must use the Service install method.

You simply select from either of the lists below the Install pushbutton and click on the Add Network Items pushbutton to select the computers or domains you want to install the Update Agent on. The computer icons that have a blue screen are computers that already have the agent installed. Computers that have a gray screen are computers that do not have the agent installed.

Installing to a Domain and a OU

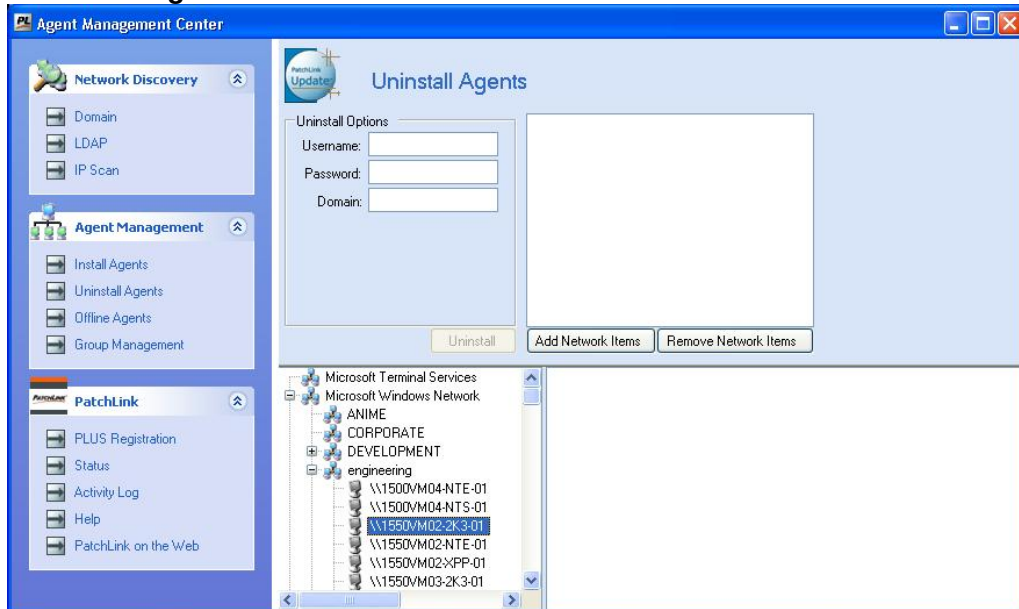


Always start from a valid Search Root, for example:

- LDAP://development
- GC:

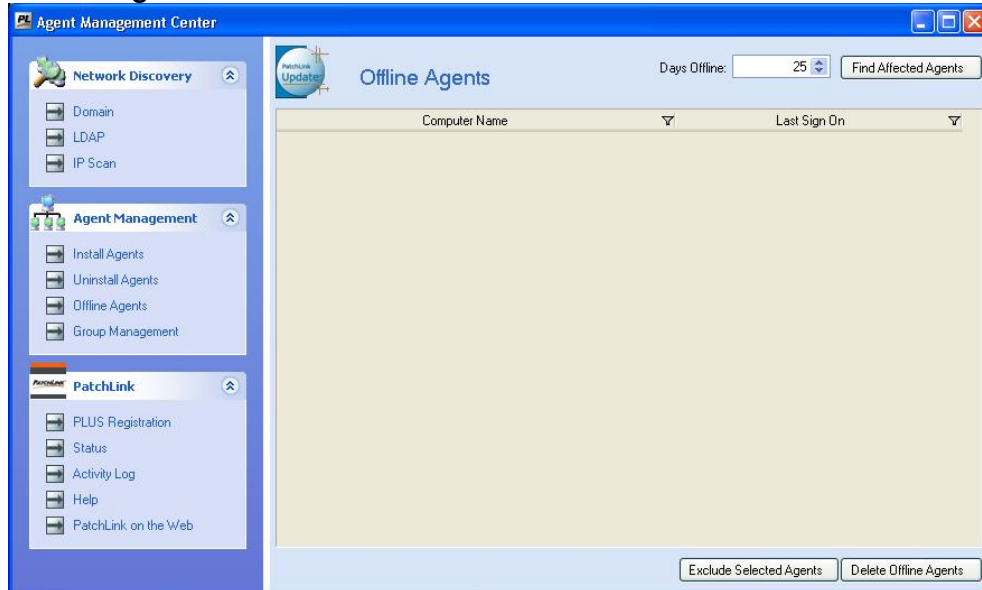
A password may or may not be needed here, depending on how security is setup in the local environment. Once a computer is found by any of the above methods, the Agent Management Center will build out the rest of the tree (parents, etc.).

Uninstall Agents Screen



The Uninstall Agents Screen allows you to uninstall agents manually. Simply select the computer(s) that you want to uninstall from one of the two lists at the bottom, select the type of uninstall, being Standard or WMI and click the Uninstall pushbutton.

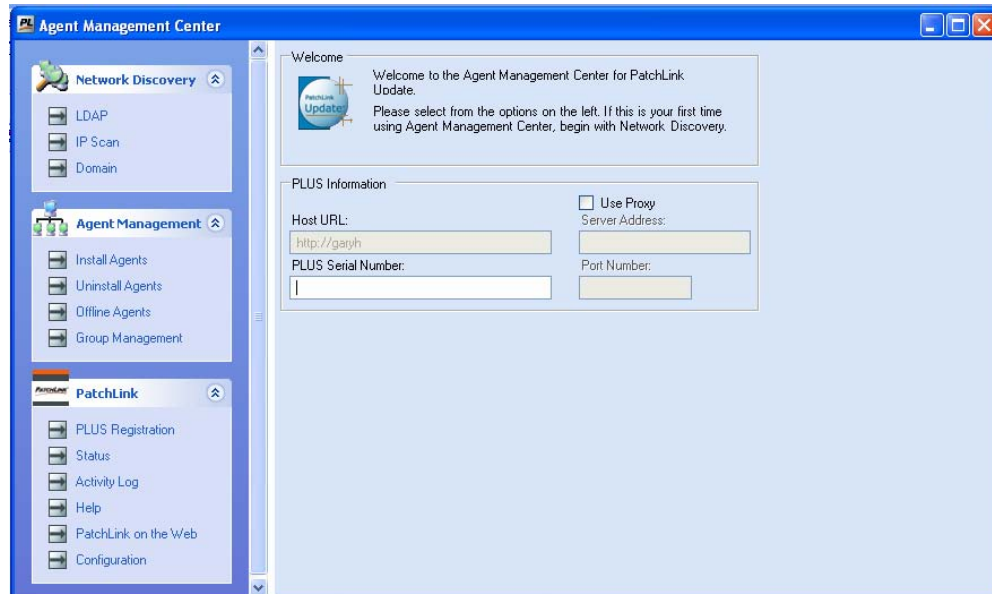
Offline Agents Screen



The Offline Agents screen allows the patch administrator to flag computers that have not registered with the PLUS server for a specific number of days that is entered in the “Days offline” screen. Computers that have been offline for more that the number of days specified in the “Days offline” field will be displayed in the gray area below the “Days offline” field.

From there you simply select the computers that you want to exclude or delete and push the appropriate pushbutton.

PatchLink Screen



The PatchLink Screen allows you to enter PLUS registration information needed to install agents, access the online help pages for the AMC and visit the PatchLink web server where you can find all the PLUS documentation as well as access to the PatchLink User Forum.

4. PatchLink Update Home Page

PatchLink Update gives you the ability to detect and patch your workstation and servers across your entire network. The **Home Page** gives you latest information and status about your PatchLink Update Server (PLUS). If PLUS licenses have expired, the License Expiration page will be displayed instead. From here you can access the PatchLink Online Documentation, Support Forum, What is PatchLink Demo, New Users page, Help Files, Known Issues and Resolutions and the PLUS Status Page.

PatchLink Update

[Home](#) | [Vulnerabilities](#) | [Inventory](#) | [Packages](#) | [Computers](#) | [Groups](#) | [Users](#) | [Reports](#) | [Options](#) | [Help](#)

Server Date & Time: 8/4/2004
2:53:54 PM (GMT-07:00)

PatchLink Online Documentation
View or download the latest online documentation.

PatchLink Support Forum
Get support and the latest information about patches....

What is PatchLink Update
Select this link to see an overview of PatchLink Update including its features and benefits...

New Users Start Here
If you are new to PatchLink Update, select this link to see how to get up and running fast...

Help Info
Select this link for full comprehensive help documentation about PatchLink Update...

Known Issues & Resolutions
Select this link to see a list of known issues and release notes about this version of the PatchLink Update Server.

PatchLink Update Server Status Page.
Select the link above to get current information on the local PatchLink Update Server.

Latest News:

DESCRIPTION
Vulnerability in Crystal Reports Web Viewer Could Allow Information Disclosure and Denial of Service (842689)

IMPACT OF VULNERABILITY: Information Disclosure and Denial of Service

May 12, 2004
Microsoft Security Bulletin MS04-015

SEVERITY: Important

DATE RELEASED: 05/12/04

Comprehensive Graphical Assessments:

Patch Status for all Computers

100.0%

Patched: 0

Partial: 0

Not Patched: 0

Detecting: 2

Pending Initial Detection: 0
Total Computers: 2

Select to Change Graph:
Patch Status for all Computers
Patch Status for all Vulnerabilities
Status for all Computers
Baseline Status for all Groups

Current Status

Company:	PatchLink: IDG-RYANH
Serial Number:	916CDB4A-94162B71
Non-Expired Licenses:	20
Licenses In Use:	2
Licenses Available:	18

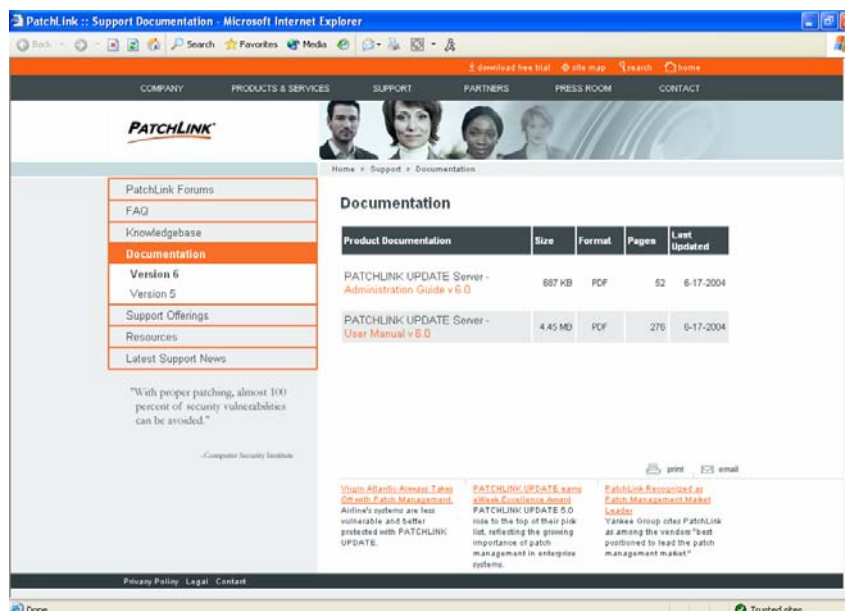
4.1 PatchLink Online Documentation

The PatchLink Online Documentation link provides a direct link to all the latest PLUS documentation. Follow the various links to provide support, forums, and resources for your PLUS.



PatchLink Online Documentation

View or download the latest online documentation.



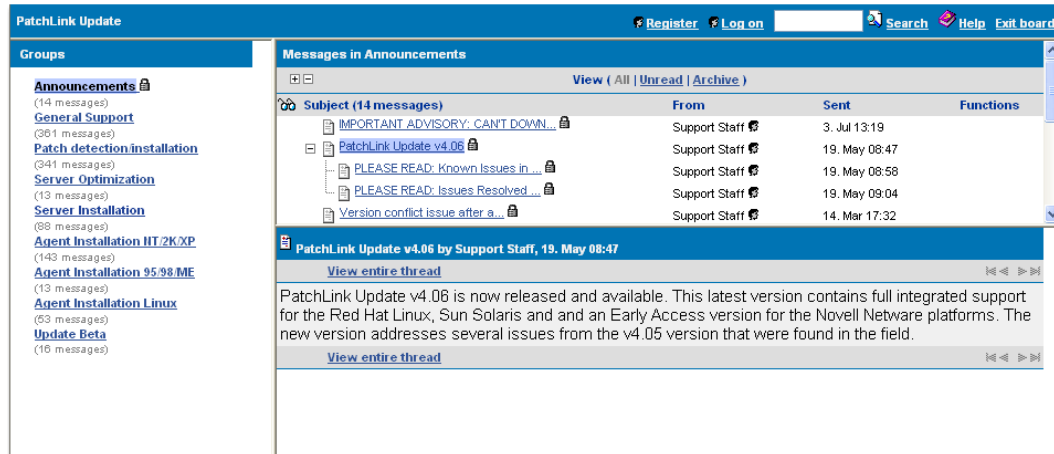
4.2 PatchLink Support Forum



PatchLink Support Forum

Get support and the latest information about patches....

The PatchLink Support Forum provides a location where the latest information and technical support about PLUS, its processes, functions and features are displayed. You can search through other customer questions and answers to see if their answers can assist you. Additionally you can post your own questions and PatchLink Customer Service will assist you in a timely manner. Registered users can select to receive notifications when any of the different forum topics receives new activity. Select the **Patchlink Support Forum** link to open the Support Forum.



- Register

Select the Register link on the Support Forum Homepage Toolbar.



You will be prompted to enter a username, a valid email address, and a password. (Remember your password; you will be prompted for it upon login) Select the password authentication options at your discretion. If you forget your password, you can have it emailed to you.

Register

Name

Email

(used for logging on)

Note: passwords are case sensitive

Password

Password again

Cancel

Register

☒ Remember my name and email

☒ Autologon (remembers password)

If you have registered already you can [log on](#)

 If you have lost your password you can [have it send to your email](#).

- Search

Enter in a keyword in the upper right hand corner text field and click on the icon to propagate the search results. For example, enter in the keyword, "UNIX" (search is NOT case sensitive.) and click on the icon.



All instances containing the word "UNIX" in its title or text appear in the results window.



Select the Search **Link** on the Support Forum Homepage Toolbar for a more detailed search.

Input a keyword, select the attributes for which to search, and select the button to initialize a more detailed search capability.

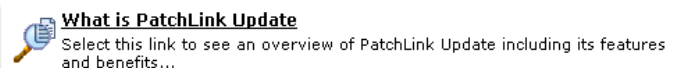
For the string

Search in	Search messages	Search the group(s)
☒ Subjects	☒ Active	☐ Search All groups
☒ Author names	☐ Archived	☒ Search only these groups
☒ Message bodies		☐ Announcements
		☐ General Support
		☐ Patch detection/Installation
		☐ Server Optimization
		☐ Server Installation
		☒ Agent Installation NT/2K/XP
		☐ Agent Installation 95/98/ME
		☐ Agent Installation Linux
		☐ Update Beta

All instances containing the selected keyword in its string appear in the results window.

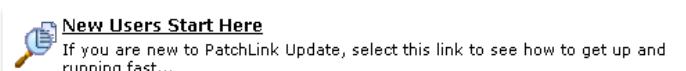
Clicking on the  icon will launch a help window for the discussion forum with specific instructions on how to navigate and participate in the discussion forums.

4.3 What is PatchLink Update?



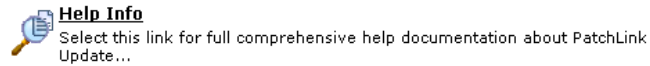
What is PatchLink Update provides a detailed overview of the **PLUS** system.

4.4 New Users Start Here



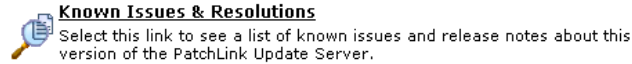
New User's Start Here displays a quick start user's guide to understanding the interface, defining access, agent behavior and their installation.

4.5 Help Info



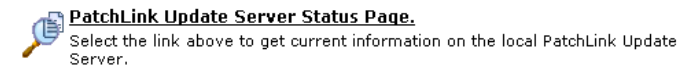
Help Info provides comprehensive documentation on PLUS.

4.6 Known Issues & Resolutions



Known Issues displays a list of Known Issues, Release Notes, and Important Links about PLUS.

4.7 PatchLink Update Server Status Page



The PatchLink Update Server Status Page shows, at a glance, the **Replication Status** between the PLUS server and the main PatchLink patch repository, PLHOST. The **Type** of replication, the **Status** of the replication, and the **Percent Complete** are displayed.

It also shows the current patch deployment **Discovery and Analysis Status**; showing whether a patch is being detected, has failed, has not started or was successful.

The **Deployment Status** portion of the page shows all deployment statuses so you can quickly check whether a package was deployed. Click on the **Deployment Name** link to view the computer's details.

[Home](#) | [Vulnerabilities](#) | [Inventory](#) | [Packages](#) | [Computers](#) | [Groups](#) | [Users](#) | [Reports](#) | [Options](#) | [Help](#)

Server Date & Time: 8/18/2004 1:53:59 PM (GMT-07:00)

Refresh

PLUS Status Page

Replication Status

Type	Status	Percent Complete
Licenses Replication	Completed	100%
Vulnerabilities Replication	Completed	100%

Discovery and Analysis Status

Status	Agent Count
Detecting	0
Failed	0
Not Started	1
Success	1

Deployment Status

Deployment Name	Total Packages in Deployment	Total Computers Assigned	Total In Progress	Total Finished	Percentage Completed
Deployment of Deployment Test and Diagnostic Package (WinXP, Win2K, Win95, Win98, WinME, WinNT, Win2K3)	1	0	0	0	0%

Cache Status

Package Name	Requested When	Step 1	Step 2	Download Start Date	Download Finish Date
PatchLink Subscription Update - To Improve Replication Time (SEE NOTES) (re-released 8/04/04)	8/17/2004 4:21:48 PM	Requested			
MS04-024 839645 (NT AD) Vulnerability in Windows Shell Could Allow Remote Code Execution	8/17/2004 4:21:48 PM	Requested			
MS04-023 840315 (NT) Vulnerability in HTML Help Could Allow Code Execution	8/17/2004 4:21:48 PM	Requested			
MS 842773 Update package that includes Background Intelligent Transfer Service (BITS) version 2.0 and WinHTTP 5.1	8/17/2004 4:21:48 PM	Requested			

The **Cache Status** is a chronological detail of your packages downloaded into the PLUS cache, including: Package Name, Requested When (Date and Time), Steps involved, Download Start Date (Date and Time), and Download Finish Date (Date and Time).

4.8 Latest News

Latest News:

Known Issues:

4.06: UK ENGLISH AUTO-UPGRADE
UK users will not be able to use the upgrade popup to upgrade the server to 4.06. Please deploy the PatchLink Update Server 4.06 -- MUST INSTALL- package from Reports like any other update or patch.

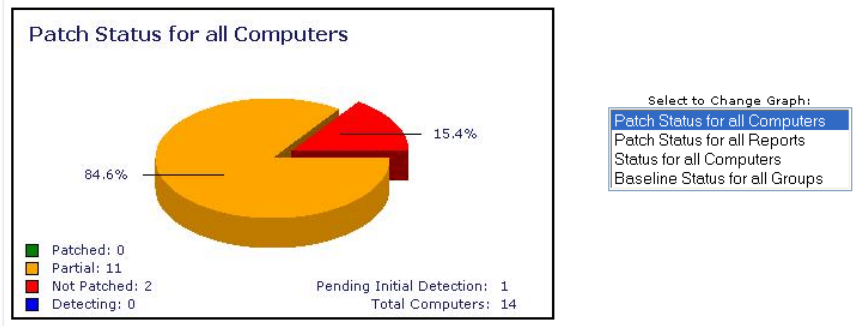
4.06: INVENTORY EXPORT TIMEOUT
If you are only retrieving partial results when clicking the "EXPORT" button, please modify your script timeout on the PLUS website from

This window displays the latest news, articles, announcements, and press releases direct from PatchLink.

4.9 Comprehensive Graphical Assessments

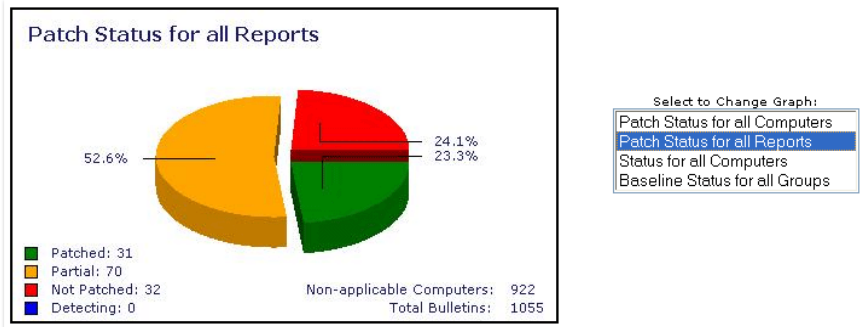
A pie chart graphical display illustrate various statuses of certain patch elements of PLUS. There are four different display views with different colors and percentages representing these various statuses. The displays are:

1. Patch Status for all Computers – displaying the status for all computers which are:



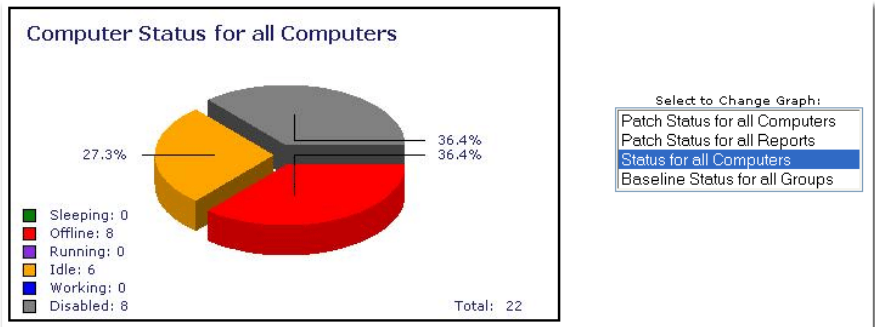
- Completely Patched
- Partially Patched
- Not Patched
- Performing the analysis detection
- Pending the initial analysis detection

2. Patch Status for all Vulnerabilities – displaying the status for all vulnerabilities:



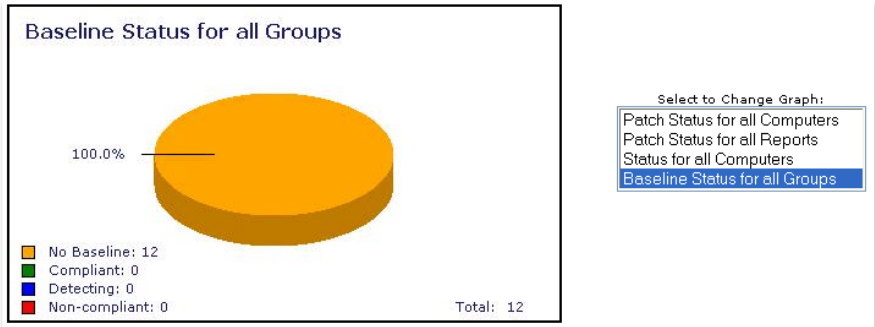
- Completely Patched
- Partially Patched
- Not Patched
- Detecting
- Vulnerabilities which have no applicable computers assigned to

3. Status for all computers:



- Sleeping (outside their hours of operation)
- Detect offline or have not communicated with PLUS in over two intervals (15 minutes minimum).
- Running: currently performing the analysis detection outside the normal means (rarely occurring when the detection process happens outside of the deployment mechanism).
- Idle: Agent is communicating fine and currently not performing any tasks.
- Working: the Agent is currently working on a task.
- Disabled and unable to perform any tasks.

4. Compliancy Status for the Mandatory Patch Baseline Status for all Groups:



- Groups whose members are fully compliant with their baseline.
- Groups whose members are not compliant with their baseline.
- Groups whose members are in the detection and analysis process.
- Groups which have no baseline.

4.10 Current Status Information

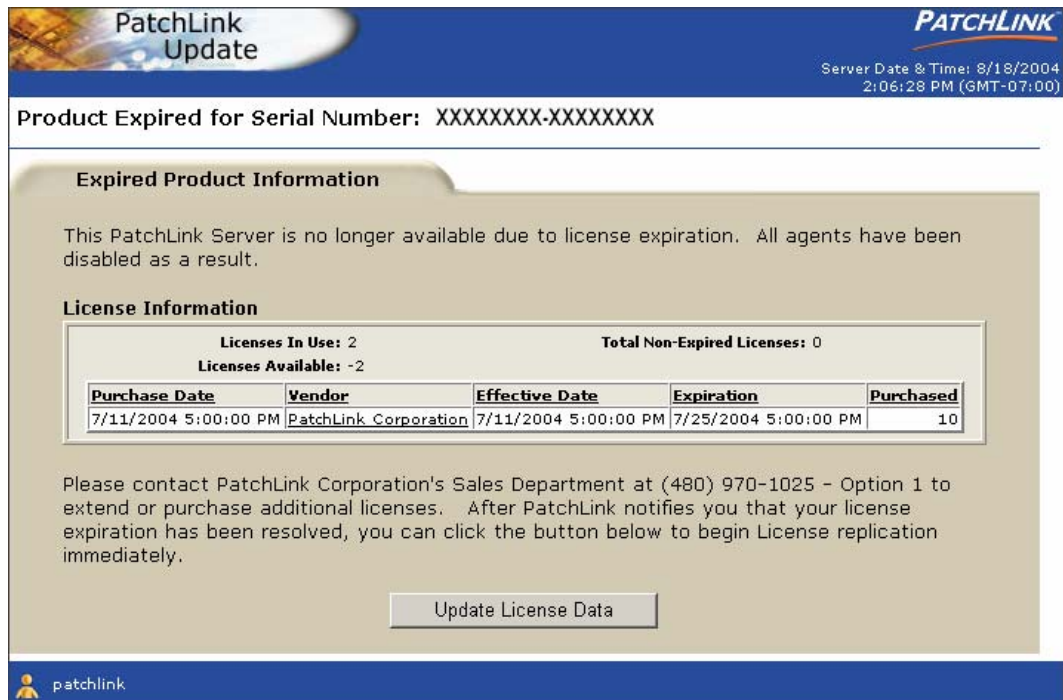
This provides you with an overall relative condition, position or state of your PLUS system.

Current Status	
Company:	SUPPORT-W2K2
Serial Number:	9942DA24-90122B71
Non-Expired Licenses:	25
Licenses In Use:	14
Licenses Available:	11
Last Update:	7/11/2003 10:07:38 AM

- Company: This is the name of the company that was entered at the time of installation.
- Serial Number: This is Your PLUS Serial Number.
- Non-Expired Licenses: This is the total number of active licenses. Each registered computer requires one license.
- Licenses in Use: This is the number of active licenses being used by registered computers.
- Licenses Available: This is the number of active and available licenses that can be used to register computers to PLUS.
- Last Update: This is the Date and Time that PLUS last updated itself from the PatchLink Host Server (PLHOST).

4.11 License Expiration

When PLUS licenses expire, the agents will no longer be able to perform any of their tasks and the home page display is replaced with this license page. Clicking the "Update License Data" button will initiate the license verification process that connects up to the PatchLink Update Host Server (PLHOST) and retrieves your updated licenses. This page will automatically refresh to the home page, once your updated licenses have been saved (this usually takes 1 minute). If you need to renew your licenses or add new licenses, please contact PatchLink Sales at 480-970-1025 Option #2.



4.12 Home Page Security

The Home Page section of PLUS requires the View Home Page access right. If a user does not have the correct access the access denied error message is displayed.

The status section of the Home Page requires the View PLUS Status access right. If a user does not have the correct access, this section is not displayed.

The ability to initiate the License Verification function requires the Manage PLUS Licenses access right. If a user does not have the correct access, the button to initiate the verification does not appear.

Contact your PatchLink Administrator (Local Super Administrator) for more information on PatchLink Update Security.

•

5. Vulnerabilities

Home | **Vulnerabilities** | Inventory | Packages | Computers | Groups | Users | Reports | Options | Help

The Vulnerabilities page is where the majority of patch management work will be performed. It contains a listing of all patch related vulnerabilities across all the systems registered to the PLUS server. It is strongly encouraged that you always manage patches from the Vulnerabilities interface, since it offers the most functionality and granularity.

A Vulnerability consists of the vulnerability description, the signatures and fingerprints required to determine whether the vulnerability is patched or not patched, and the associated package or packages for performing the patch.

5.1 Vulnerability Analysis

This section displays the analysis results from the Discover Applicable Updates process on each computer. The analysis gives a simple top-down view of vulnerability patch status. The total number of vulnerabilities is displayed just above the table in the top right corner.

The Vulnerability Analysis can be viewed at the network level, for computer groups, and for individual computers. The various statuses are detailed in this section.

The screenshot shows the 'Vulnerabilities' page in the PatchLink interface. At the top, there's a navigation bar with 'Home | Vulnerabilities | Inventory | Packages | Computers | Groups | Users | Reports | Options | Help'. Below this, a search bar is labeled 'Vulnerability Analysis' with a search input field and a 'Status' dropdown set to 'Patched'. There are also 'Results for Groups' and 'Impact' dropdowns. A 'Save as Default View' checkbox and an 'Update View' button are present.

The main section is titled 'Vulnerabilities' and shows a table with 122 total items. The table has columns for 'Vulnerability Name', 'Impact', and a series of status indicators (1, 0, 0, 0, 1, 100%). The vulnerabilities listed include:

- C - PatchLink Update Agent HotFix 5.0.1.60 --MUST INSTALL--
- MS 841720 Sasser Worm Removal Tool (Version 4.0)
- MS 870669 Disable the ADOBE.Stream object from Internet Explorer (SEE NOTES)
- MS 873018 Download.Ject Worm Existence and Removal Tool (Version 1.0)
- MS04-016 839643 Vulnerability in DirectPlay Could Allow Denial of Service
- MS04-018 823353 Cumulative Security Update for Outlook Express 6 SP1
- MS04-019 842526 Vulnerability in Utility Manager Could Allow Code Execution

At the bottom, there's a toolbar with buttons: 'View', 'Deploy', 'Disable', 'Lock', 'Unlock', 'Export', 'Scan Now', and 'Update Cache'.

Clicking the plus sign next to a vulnerability will display the detailed results of the analysis. The same detailed results are displayed when you place a checkmark in the box next to the vulnerability and click on the **View** button.

Vulnerability Analysis

Search (vulnerability name/CVE no.): Status: **Not Patched**

Results for Groups: **All** Impact: **All**

Save as Default View: ☐ Update View

Vulnerability Status **Package Status** **Filters** **Impact Categories** **Statistics**

Vulnerabilities **Vulnerability Name** **Impact** **Statistics**

Microsoft .NET Framework 1.1 SP1 Critical 0 1 0 0 1 100%

Type: Active Vulnerability Analysis
Impact: Critical
Status: Enabled
Downloaded On: 9/16/2004 7:49:10 PM (GMT-07:00)
Associated Distribution Packages: 2
Distribution Packages Status: Cached and ready for deployment.
Vendor: [Microsoft Corp.](#)
Released On: 4/8/2003 5:00:00 PM (GMT-07:00)
Vendor Product ID: NDP113P867460

Report Details

Common Vulnerability Exploit (CVE): CAN-2004-0200
Vulnerability Code Description:
Reference Text:

Description: The primary focus of Microsoft .NET Framework 1.1 Service Pack 1 (SP1) is improved security. In addition, the service pack includes roll-ups of all reported customer issues found after the release of the Microsoft .NET Framework 1.1. Of particular note, SP1 provides better support for consuming WSDL documents, Data Execution Prevention and protection from security issues such as buffer overruns.

SP1 also provides support for Windows XP Service Pack 2 to provide a safer, more reliable experience for customers using Windows XP. [More Information](#)

Expand Bulletin

	Impact	0	1	0	0	2	100%
MS04-018 823353 Cumulative Security Update for Outlook Express 5.5 SP2	Critical	1	1	0	0	2	100%
MS04-018 823353 Cumulative Security Update for Outlook Express 6 SP1	Critical	0	2	0	0	2	100%
MS04-019 842526 Vulnerability in Utility Manager Could Allow Code Execution	Critical	1	2	0	0	3	100%
MS04-025 867801 Cumulative Security Update for IE 6.0	Critical	1	1	0	0	2	100%
MS04-025 867801 Cumulative Security Update for IE 6.0 SP1	Critical	0	1	0	0	1	100%
MS04-028 833987 Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution	Critical	0	1	0	0	1	100%
Patchlink Subscription Update - To Improve Replication Time (SEE NOTES) (re-released 8/04/04)	Critical	0	3	0	0	3	100%

• Vulnerability Status & Types



The status of a vulnerability is indicated by the following icons:

Beta	New	Current	Status Description
			This is an active vulnerability.
			This vulnerability has been locked and is in compliance.
			This vulnerability has been locked and is out of compliance.
			This vulnerability has been disabled.

Additional information about the status of the associated distribution package is displayed upon hovering your mouse pointer over the icon.

- Beta: This vulnerability has been released to the BETA community of PatchLink.
 - New: This vulnerability has been downloaded from PLHOST and has arrived since you started your PLUS session.
 - Current: This is a current vulnerability that has been downloaded from PLHOST before you started your PLUS session.
- Package Cache Status & Types



A vulnerability may have any number of distribution packages associated with it. A distribution package contains the patch to fix the vulnerability. Each distribution package may be cached (downloaded) from the PatchLink Update Host Server (PLHOST) to PLUS. They may be cached automatically if the vulnerability's impact is critical or if a deployment has been created to deploy the package(s). The package cache status icon is a hyperlink. By clicking on the icon, you will initialize a list of the individual packages that are associated with that vulnerability.

Current	New	Status Description
		At least one of the packages is being deployed.
		The packages are cached and ready for deployment.
		At least one of the packages is being cached from PLHOST.
		At least one of the packages has not been cached.

Additional information about the status of the associated distribution package is displayed upon hovering your mouse pointer over the icon.

- New: This distribution package has been released and its metadata has been downloaded from PLHOST since you began your PLUS session.
- Current: This distribution package has been released and its metadata has been downloaded from PLHOST before you began your PLUS session.

5.2 Vulnerability Impact



The agent list initially sorts by Impact alphanumerically in ascending order. To sort by another field (other than vulnerability or package status) click on the field name. To reverse the alphanumeric sort from ascending to descending, click on field name again.

- **Critical**
The manufacturer or PatchLink has determined that this patch is critical and should be installed as soon as possible. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on the PatchLink Update Server.
- **Critical - 01**
The manufacturer or PatchLink has determined that this patch is critical and should be installed as soon as possible. The patches for this category are older than 30 days and are not automatically downloaded and stored.
- **Critical - 05**
These vulnerabilities have been superceded by more recently released vulnerabilities. The patches for this category are not automatically downloaded and stored.
- **Critical – Intl**
These vulnerabilities include patches for non-English operating systems, which the manufacturer or PatchLink has determined are critical and should be installed ASAP. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on the PatchLink Update Server.
- **Recommended**
The manufacturer or PatchLink has determined that this patch, while not critical or security related is useful and should be applied to maintain the health of your computers.
- **Informational**
The manufacturer or PatchLink has determined that this patch is useful, though does not contain any changes that are necessary for day to day operations. Documentation updates are an example of the patches in this category.
- **Detection-Based**
These vulnerabilities contain signatures that are common to multiple vulnerabilities. They contain no associated patches are only used in the detection process.
- **Software**
This category contains software updates. These vulnerabilities contain the fingerprints and signatures to determine whether the prerequisites are met for the installation of these applications.
- **Task**
This category contains tasks which administrators may use to run various detection or deployment tasks across their network.
- **Security**
These vulnerabilities detect common security concerns, problems and configuration issues. While these vulnerabilities do not necessarily involve an associated patch to fix them, they have associated packages (or packages) which assist in resolving the problems.

- Virus Removal
These vulnerabilities detect and remove viruses and worms.

5.3 Statistics

The right-hand side of the vulnerability entry contains columns which illustrate the current result statistics for the computers which have been scanned in addition to the overall percentage completion of all computers which will be scanned for that particular vulnerability.

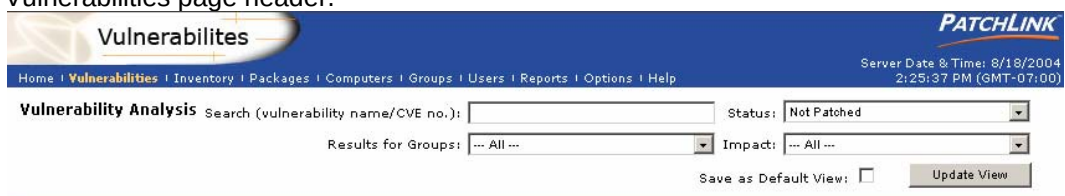


Result	Result Definition
	Total number of computers that are patched.
	The total number of computers that are not patched.
	The total number of computers that produced an error while determining the patch status for the vulnerability.
	The total number of computers that are still waiting for the vulnerability analysis to finish.
	The total number of computers that have met the prerequisites for the vulnerability.
	The percentage of computers that have finished the vulnerability analysis.

You may sort by Ascending (default view) or Descending order by clicking on the corresponding results definition icon.

5.4 Page Functions

- Display and Hide
Click the to display additional information and statistics about the represented item.
Click the to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (,) is only available for Microsoft Internet Explorer at this time.
- Advanced Page Search, Filtering, and View Saving
The advanced page search, filtering dropdown menus, and saving functions appear in the Vulnerabilities page header.



- **Search**

Search (vulnerability name/CVE no.):

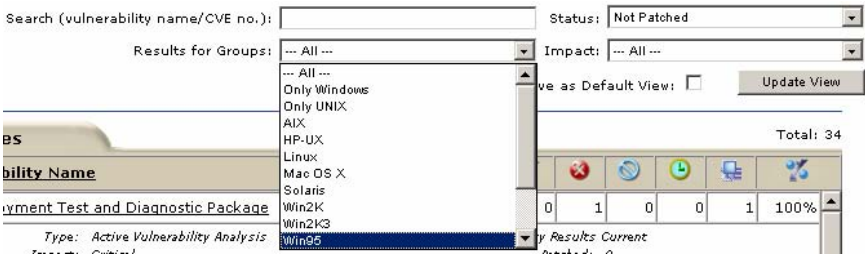
You may search vulnerabilities for more granular results by entering the vulnerability name (CVE; Common Vulnerabilities and Exposures) text into the **Search** field and clicking on the Update View button.

This will return the vulnerabilities having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- **Results for Groups**

Filter by **Groups** using the dropdown menu and click on the Update View button.

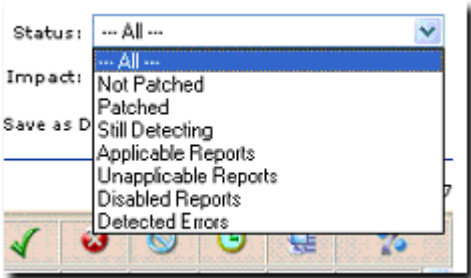


This will return the vulnerability having the selected group. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- **Status**

Filter by Vulnerability Status using the dropdown menu and click on the Update View button.

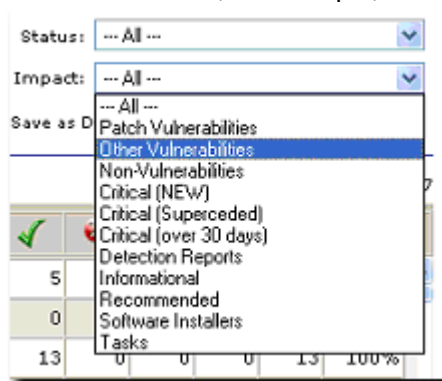


This will return the vulnerabilities having the selected status. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

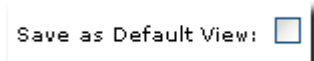


- **Impact**
Filter by vulnerability impact using the dropdown menu and click on the Update View button.

This is extremely useful when you want to find or display only the vulnerabilities that, for example, are Critical (NEW).



This will return the vulnerabilities having the selected impact. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- **Sort**
The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.
- **Mouse Overs**
Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.
- **Checkboxes**
Checkboxes are used to either select a single item or a group of items to initialize them for a certain function. Checkboxes appear throughout the PLUS and are **not** visible in Netscape.

5.5 Action Menu

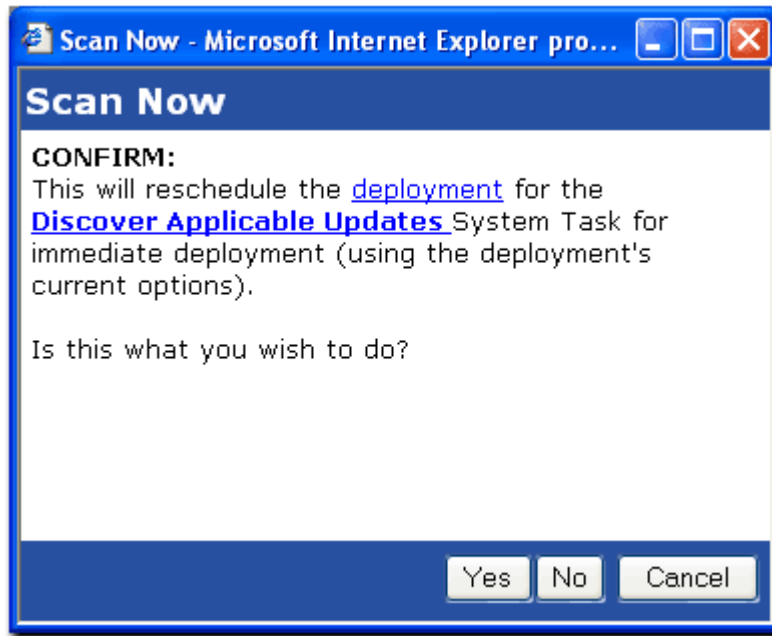


- **View**
The vulnerabilities filter controls which vulnerabilities are displayed. There are three options to choose from: Vulnerabilities that have computers applicable to them, Disabled Vulnerabilities or view All Vulnerabilities.

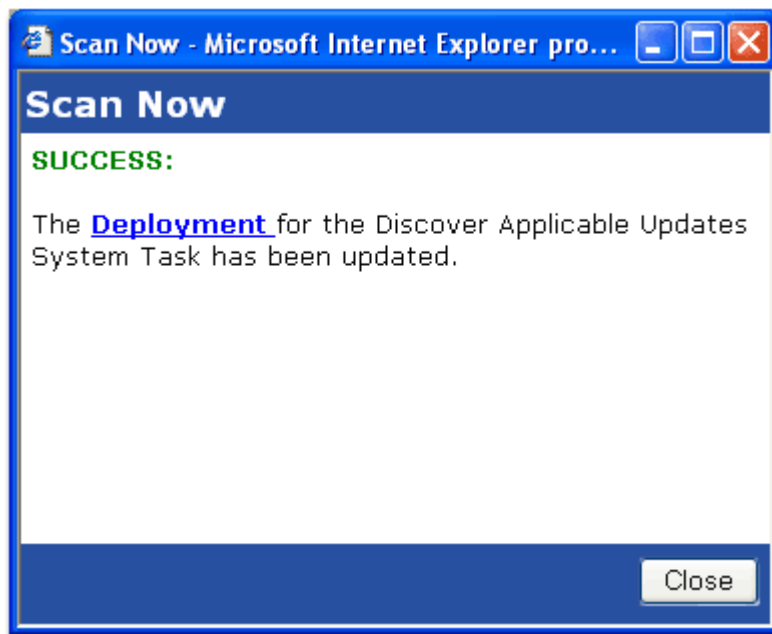
- **Deploy**
This creates a deployment for the selected vulnerability. [See Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information.
- **Disable**
This removes the selected enabled vulnerabilities from being able to be scanned during the Discover Applicable Updates process from all levels of the system (network level down to the individual computer level).
- **Enable**
This re-enables the scanning ability for the selected disabled vulnerabilities during the Discover Applicable Updates process.
- **Lock**
Selecting a vulnerability and clicking on the lock button will save the current vulnerability analysis values. When the analysis is again displayed this data is compared to the current data to determine if the vulnerability is in or out of compliance. If the vulnerability is out of compliance, it is highlighted in red.
- **Unlock**
Selecting a locked vulnerability and clicking on the unlock button will clear out the vulnerability's locked data.
- **Export**
Export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to all selected computers.

To initialize (choose) all computers, click on **Scan Now** button without selecting any computers.

If you choose not to select any computers, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the computers.



To reschedule the **Discover Applicable Updates**, select Yes



PLUS will reschedule the selected computer(s), initialize a screen stating its success and provide a deployment link to initialize a new screen with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Computers page will be refreshed. Previously selected deployment options are maintained.

- **Update Cache**
Update Cache initiates the process to cache (or re-cache) the associated distribution packages for the selected vulnerability.

5.6 Vulnerability Analysis Security

*The Vulnerabilities section of PLUS requires the **View Vulnerabilities Page** access right. If a user does not have the correct access the access denied error message is displayed.*

*To be able to view the detailed vulnerability analysis requires the **View Vulnerability Details** access right. If a user does not have the correct access, the hyperlink will not be shown and the **View** button is disabled.*

*To be able to change the filter from detected vulnerability to disabled or all requires the **Change Vulnerability Filter** access right. If a user does not have the correct access, the filter will not have any options to choose from.*

*To be able to view the associated distribution packages for a given vulnerability requires the **View Packages** access right. If a user does not have the correct access, the link on the package status image is disabled.*

*To be able to create a deployment based on the vulnerability analysis requires the **Deploy Vulnerabilities** access right. If a user does not have the correct access, the **Deploy** button is disabled.*

*To be able to enable or disable vulnerabilities from being available by the Discover Applicable Updates process requires the **Manage Vulnerabilities** access right. If a user does not have the correct access, the **Enable** and **Disable** buttons are disabled.*

*To be able to lock or unlock the selected vulnerabilities requires the **Manage UI Vulnerability Locks** access right. If a user does not have the correct access, the **Lock** and **Unlock** buttons are disabled.*

*To export all of the vulnerability analyses to a comma-separated value (CSV) file requires the **Export Vulnerability Data** access right. If a user does not have the correct access, the **Export** button is disabled.*

*To restart the Discover Applicable Updates process for all of the computers registered to the PLUS requires the **Manage System Tasks** access right. If a user does not have the correct access, the **Scan Now** button is disabled.*

*To cache the associated distribution of the selected vulnerabilities requires the **Cache Packages** access right. If a user does not have the correct access, the **Update Cache** button is disabled.*

5.7 Vulnerability Analysis Details

The Status data for each vulnerability is based on your unique configuration of systems. By clicking the vulnerability link, a full list of all computers that require the patch in question will be displayed. From there, the patch can be easily deployed.

From the Vulnerabilities page, click on the **Vulnerability Name Link** to view the computer-level analysis of the vulnerability.

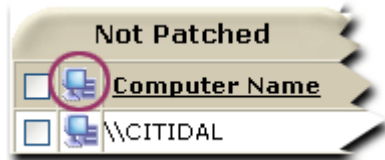
The analysis results of the vulnerability are detailed and separated into four tabbed displays. The name of the tab represents status for those computers in the vulnerability analysis.

Reports					PATCHLINK
Home Reports Inventory Packages Computers Groups Users Options Server Times: 6/4/2003 12:43:11 PM (GMT-)					
MS03-008 814078: Flaw in Windows Script Engine could allow code execution					
Not Patched Patched Error Detecting Total Computers: 5					
Computer Name	Other Name	Operating System	OS Version	Analysis Date	
\\DANV	DanV.patchlink.com	WinXP	WinXP-Service Pack 1	6/3/2003 7:58:17 PM	
\\IDG-PLUS-01	idg-plus-01.patchlink.com	Win2K	Win2K-Service Pack 2	6/3/2003 7:58:37 PM	
\\IDG-VSS-01	idg-vss-01.patchlink.com	Win2K	Win2K-Service Pack 2	6/3/2003 7:59:40 PM	
\\JONG	JonG.patchlink.com	WinXP	WinXP-Service Pack 1	6/3/2003 7:56:53 PM	
\\SAMEERJ	SameerJ.patchlink.com	WinXP	WinXP	4/26/2003 10:34:16 AM	

patchlink_help | Deploy | View Package | Export

- Analysis Results
 - Not Patched: These computers were detected as needing the vulnerability patch.
 - Patched: These computers were detected as being patched for the vulnerability.
 - Error: These computers produced an error while determining the patch status for the vulnerability.
 - Detecting: These computers are either in the process of determining the patch status for the vulnerability or waiting for the detection and analysis process to begin.

5.8 Agent Status



Status	Description
	The agent is sleeping as it is outside of its hours of operation.
	The agent has not contacted PLUS in more than 2 intervals (minimum of 15 minutes for intervals smaller than 10 minutes). It is considered to be offline.
	This is an active detection agent that does not correspond to a registered deployment agent
	This is an active deployment agent.
	This agent has been disabled.

Additional information may be displayed by hovering your mouse pointer over the icon.

- Agent Information
 - Host Name: This displays the name of the computer.
 - Other Name: This displays either the DNS name for the computer or its IP address if it does not have an assigned DNS name.
 - Operating System: This displays the abbreviated the operating system name
 - OS Version: This displays additional operating system version information.
 - Last Reported Date: This is the date the agent last ran the Discover Applicable Updates process.

5.9 Action Menu



- Deploy

This invokes the Deployment Wizard and allows you to create a deployment for the selected vulnerability. [See Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information.
- View Package

This displays the associated distribution packages for the vulnerability.
- Export

Export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is selected and sorted on.

5.10 Vulnerability Analysis Security

The Vulnerability Analysis Details section of PLUS requires the [View Vulnerability Details](#) access right. If a user does not have the correct access the access denied error message is displayed.

To be able to create a deployment based on the vulnerability analysis requires the [Deploy Vulnerabilities](#) access right. If a user does not have the correct access, the [Deploy](#) button is disabled.

To be able to view the associated distribution packages for a given vulnerability requires the [View Packages](#) access right. If a user does not have the correct access, the [View Package](#) button is disabled.

To export the vulnerability analysis to a comma-separated value (CSV) file requires the [Export Vulnerability Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

6. Inventory

Home | Vulnerabilities | **Inventory** | Packages | Computers | Groups | Users | Reports | Options | Help

PLUS has the capability to determine what patch is applicable to what machine and has strong inventory capabilities for all the software, hardware, operating system and services on a system. The inventory reports all Operating System, Installed Software, Hardware and their device drivers, and Services from a network perspective down to the single machine level.

Clicking the will display the list of computers containing this inventory item. Clicking the will hide this list from view. The computer list is refreshed each time it is displayed. The alternative method to obtain this list is to click on the name of the inventory item and the page will be refreshed with this list.

Inventory Summary

Search (inventory name): Groups: Type:

Save as Default View: ☐

Inventory Total: 2311

Software Programs	Count
4Suite 0.11 Python tools and libraries for XML processing and databases.	1
4Suite 0.11.1 Python tools and libraries for XML processing and databases.	2
a2ps 4.13b Converts text and other types of files to PostScript(TM).	2
abiword 0.7.14 A word processor.	1
abiword 0.99.5 A word processor.	1
ac-archive 0.5.39 autoconf extensions archive	1
acl 2.2.3 Access control list utilities.	1
adjtimex 1.13 A utility for adjusting kernel time variables.	1
alchemist 1.0.18 A multi-sourced configuration back-end.	1
alchemist 1.0.23 A multi-sourced configuration back-end.	1
alchemist 1.0.26 A multi-sourced configuration back-end.	1
alchemist-devel 1.0.18 Files needed for developing programs which use alchemist.	1
alchemist-devel 1.0.23 Files needed for developing programs which use alchemist.	1
alchemist-devel 1.0.26 Files needed for developing programs which use alchemist.	1

patchlink

Done Internet

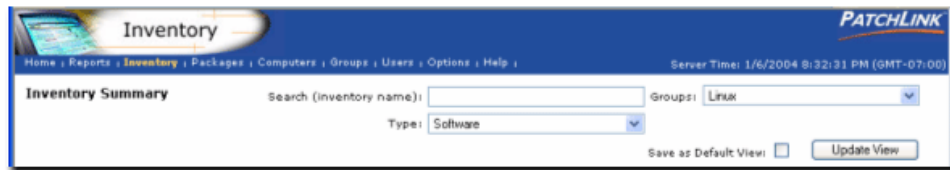
6.1 Page Functions

- Display and Hide

Click the  to display additional information and statistics about the represented item. Click the  to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (, ) is only available for Microsoft Internet Explorer at this time.

- Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Inventory Summary page header.

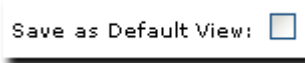


- Search



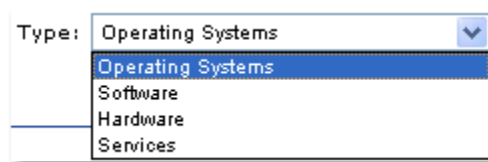
You may search inventory for more granular results by entering the inventory name text into the **Search** field and clicking on the  **Update View** button.

This will return the inventory having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- Type

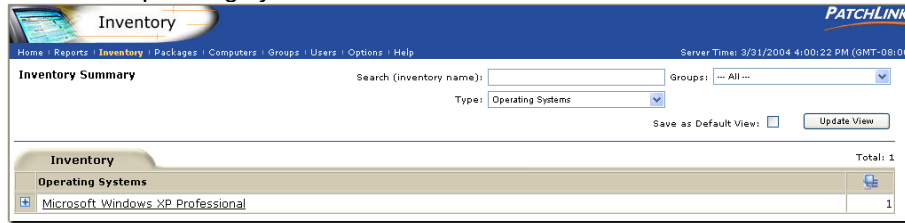
Filter by Type using the pull down menu and click on the  **Update View** button.



This allows you to search for Operating Systems, Software, Hardware and Services.

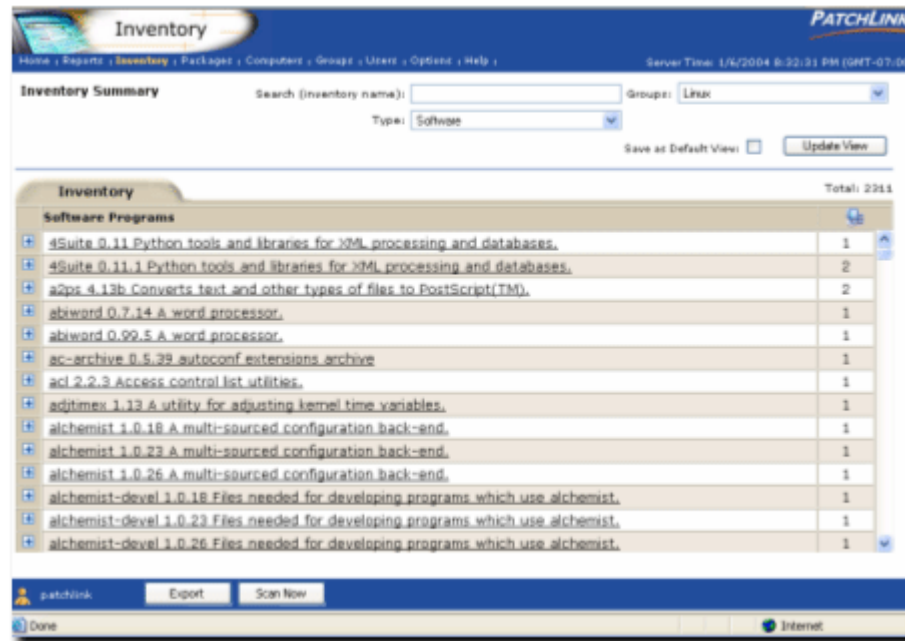
Operating Systems View

Displays the full operating system platform names and the number of instances, or times this operating system was detected.



Software View

Displays the installed software applications and the number of instances, or times this software application was detected.



Software Programs

This displays the name of the software application. Click the for a software application to display the list of computers for that application. Click on the to close this list.

Number of Instances

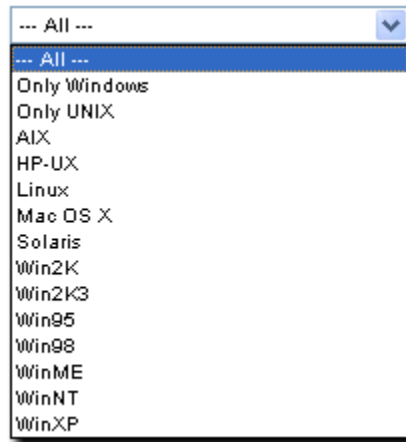
The number of times this software application was detected.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

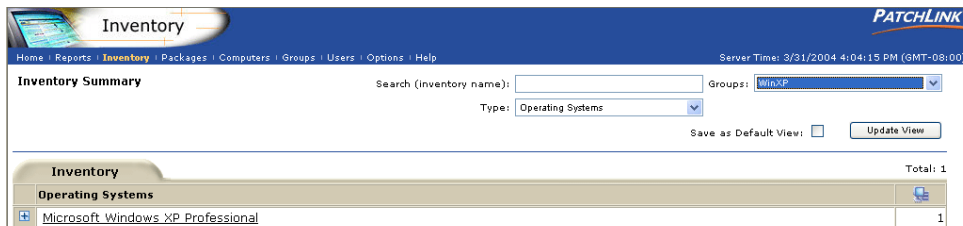
Save as Default View: ☐

- Groups

Filter by Group using the pull down menu and click on the  Update View button.



This allows the user to search on any user defined or server defined groups that exist.

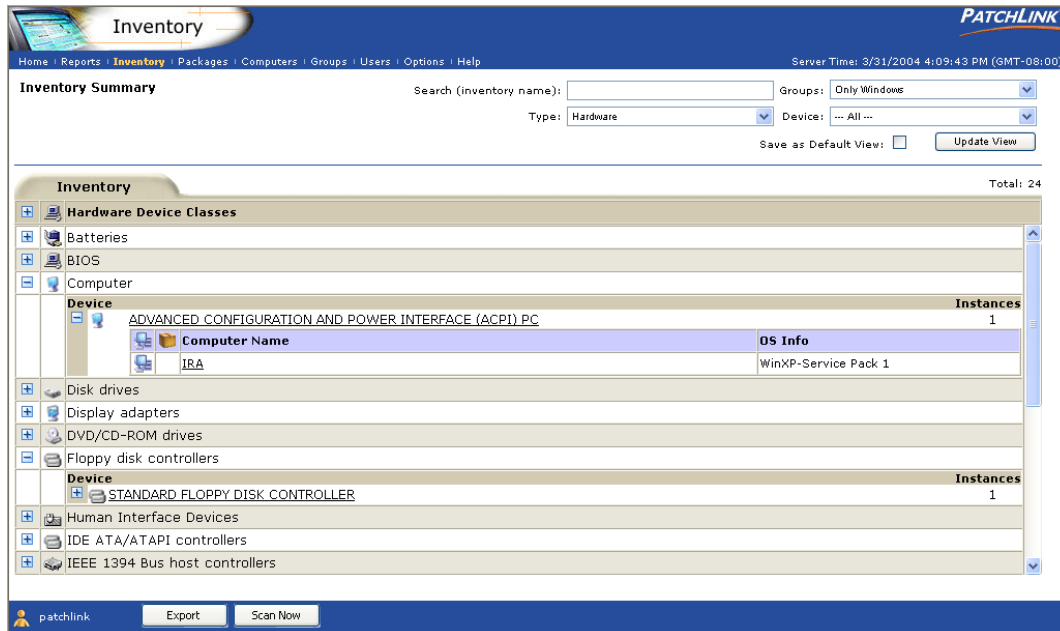


- o Operating Systems
Displays the selected or filtered operating system.
- o Number of Instances
This displays the number of times this operating system platform has been detected. For displaying the Operating System Inventory for a single computer, this is always one.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

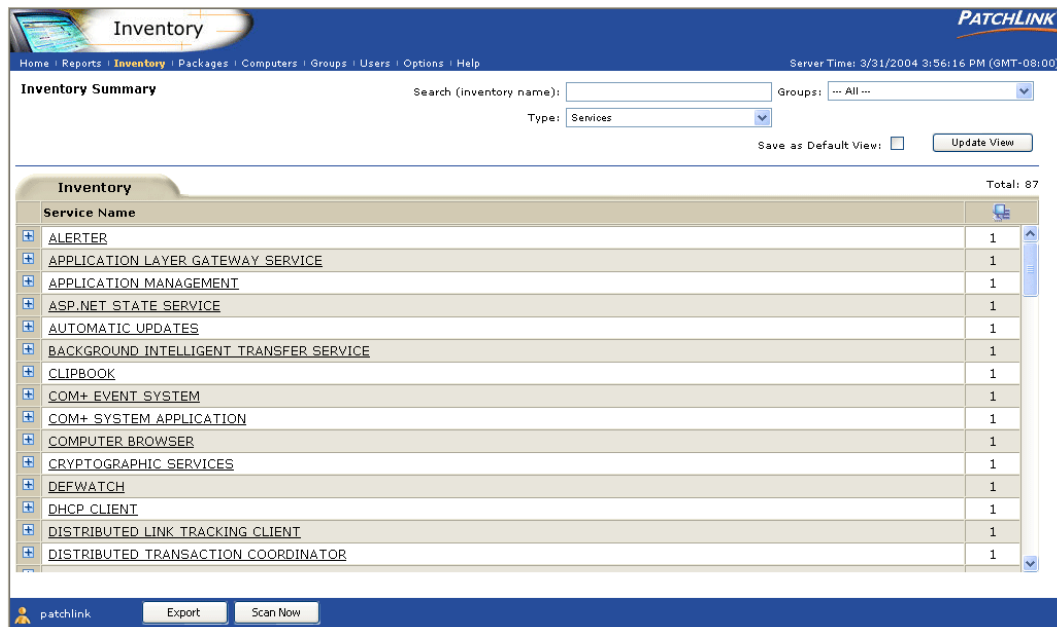
Save as Default View: ☐

- **Hardware View**
Displays the client Hardware devices.



- o **Hardware Device Class**
Hardware is separated into device classes such as disk drives, processors, network adapters, etc. Click the to display the list of devices for each class, or click on the to display them all (for a long list of devices this may take a few moments to generate). Click the to close this list.
- o **Device**
A device is a specific piece of hardware, such as a "Microsoft USB IntelliMouse Optical". Click the for a device to display the list of computers for that device. Click the to close this list.
- o **Number of Instances**
An Instance is a specifically detected device or installed driver. A computer may contain multiple instances of a installed device or driver. For example, a computer may contain a video graphics adapter that contains multiple video sources and destinations in which each source or destination is discovered as multiple instances of the same device or driver.

- **Services View**
Displays the detected services that may or may not be running.



- o **Service Name**
This displays the name of the service.
- o **Number of Instances**
The number of times this service was detected.

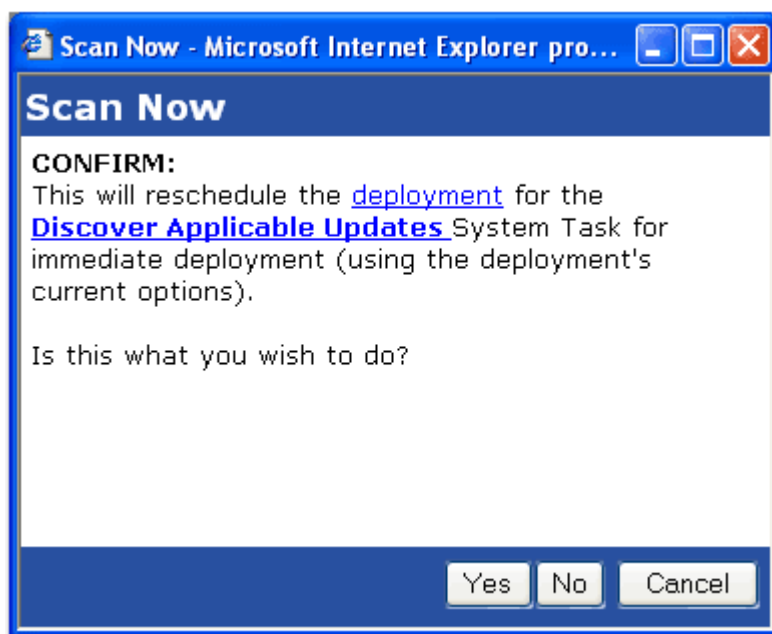
6.2 Action Menu



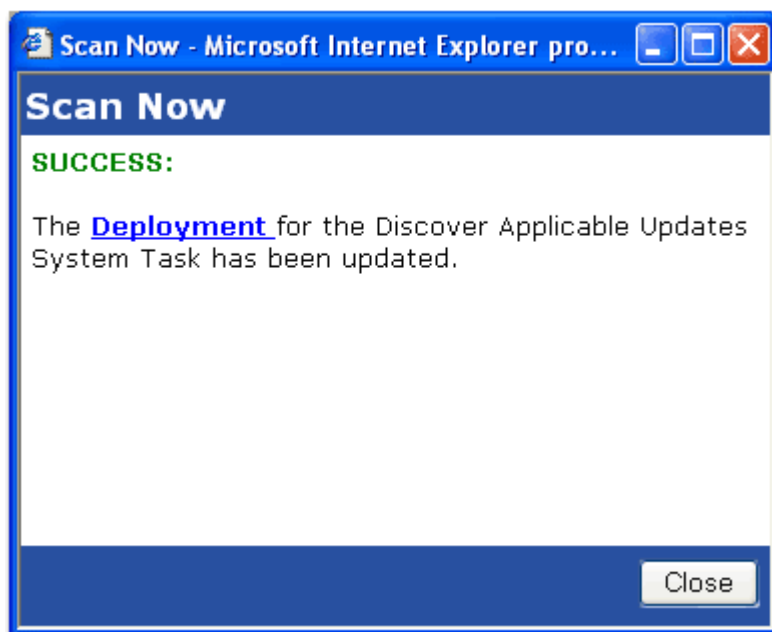
- **Export**
Export the filtered inventory data to a comma-separated value (CSV) file.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected computers.

To initialize (choose) all computers, click the **Scan Now** button without selecting any computers.

If you choose not to select any computers, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the computers.



To reschedule the **Discover Applicable Updates**, select Yes.



PLUS will reschedule the selected computer(s), initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the pop-up window, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

6.3 Discovered Inventory Security

*The Inventory section of PLUS requires the **View Inventories** access right. If a user does not have the correct access the access denied error message is displayed.*

*To be able to view the **Software** inventory requires the **View Software Inventories** access right. If a user does not have the correct access, the filter will not have this option available.*

*To be able to view the **Hardware** inventory requires the **View Hardware Inventories** access right. If a user does not have the correct access, the filter will not have this option available.*

*To be able to view the **Services** inventory requires the **View Services Inventories** access right. If a user does not have the correct access, the filter will not have this option available.*

To be able to view the list of computers on which an inventory belongs to requires the View Computers access right. If a user does not have the correct access, the hyperlink on the inventory item is not disabled and the  function is disabled.

*To export the inventory to a comma-separated value (CSV) file requires the **Export Inventory Data** access right. If a user does not have the correct access, the **Export** button is disabled.*

7. Packages

Home | Vulnerabilities | Inventory | **Packages** | Computers | Groups | Users | Reports | Options | Help

Distribution Packages contain all the actual patch software and executable code used for patch deployment. Vulnerabilities may contain several patch packages that will be deployed in a specific order. You can create custom packages from this page that do not require the patented PatchLink Fingerprinting technology. The ability to create custom packages demonstrates the software distribution capabilities of PatchLink Update Server as well as other tasks that you may require.

Distribution packages will contain whatever you want to deploy on a computer or group. A distribution package can run tasks or scripts, install software applications, place files (or directories of files) to a specified location, change the configuration of an application or service, or various other things that can be done in an unattended manner. The majority of the packages contain the patches for vulnerabilities, defects or bugs. If you would like to create your own patch, application or script package, see [Section 8; Creating and Editing Packages: Package Editor Wizard](#) and [Section 9: Deploying Packages: Schedule Deployment Wizard](#) for more information on custom packages.

The screenshot shows the 'Packages' page in the PatchLink interface. At the top, there's a navigation bar with 'Home | Reports | Inventory | **Packages** | Computers | Groups | Users | Options | Help'. Below this, a search bar allows filtering by 'Search (package name):' and 'Status: --- All ---'. There's also a dropdown for 'Operating System: --- All ---'. A 'Save as Default View' checkbox and an 'Update View' button are present.

The main section is titled 'Enabled Packages' and shows a table of 46 packages. The table has columns for 'Package Name', 'Origin', 'Operating Systems', and a count. The packages listed include Citrix ICA Win32 Client, Command Anti-Virus DEF files, Computer Associates DAT files, Discover Applicable Updates, F-Prot Antivirus DEF files, IBM AIX maintenance package, and McAfee AntiVirus DAT file.

Package Name	Origin	Operating Systems	Total: 46
Citrix ICA Win32 Client - v7.1	PatchLink	Win95, Win98, WinME, WinNT, WinXP	0
Command Anti-Virus DEF file for v4.6x or lower (April 01, 2004)	PatchLink	Win2K, WinXP	0
Command Anti-Virus DEF file for v4.6x or lower (April 01, 2004)	PatchLink	Win95, Win98, WinME, WinNT	0
Command Anti-Virus DEF file for v4.7x or higher (April 01, 2004)	PatchLink	Win95, Win98, WinME, WinNT, Win2K, WinXP, Win2K3	0
Computer Associates DAT file 11.4.8254 for eTrust Antivirus Vet Engine (April 2, 2004)-a	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
Computer Associates DAT file 11.4.8254 for eTrust Antivirus Vet Engine (April 2, 2004)-b	PatchLink	Win95, Win98, WinME	0
Computer Associates DAT file 23.64.59 for eTrust Antivirus InoculateIT Engine (April 2, 2004)-a	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
Computer Associates DAT file 23.64.59 for eTrust Antivirus InoculateIT Engine (April 2, 2004)-b	PatchLink	Win95, Win98, WinME	0
Discover Applicable Updates	System	Win95, Win98, WinME, WinNT, Win2K, NetWare, Linux, WinXP, Solaris, Win2K3, AIX, HP-UX	1
F-Prot Antivirus DEF files for Application/Script viruses and Trojans (April 01, 2004)	PatchLink	Win95, Win98, WinME, WinNT, Win2K, WinXP, Win2K3	0
IBM AIX 4330(05/06/07)-11: Recommended Maintenance Package	PatchLink	AIX	0
McAfee AntiVirus DAT file 4346 for VirusScan 6.x and 7.x (March 31, 2004)	PatchLink	Win95, Win98, WinME, WinNT, Win2K, WinXP, Win2K3	0

At the bottom, there's a toolbar with buttons: View, Deploy, Add, Change, Remove, Export, and Update Cache.

7.1 Package Information

- **Package Name**
This displays the name of the distribution package. Clicking on the distribution package will display the deployments for that distribution package.

The package and Deployment details are as follows:
 - Distribution Package Name
 - Origin
 - Status
 - Cache Status
 - Cache Request Status
 - Deployment Availability
 - OS Platforms
 - The user who created this distribution package
 - The date the distribution package was created
 - The user who last modified the distribution package
 - When the distribution package was last modified
 - The date when a deployment was last created for this distribution package
 - Version
 - Total number of directories found in the package
 - Total number of files found in the package
 - Total size of the compressed package size (in KB)
 - Total number of prescripts
 - Total number of postscripts
 - Total number of command-line scripts
 - Total number of dependant distribution packages
 - Total number of idle deployments
 - Total number of running deployments
 - Total number of deployments that failed
 - Total number of deployments that were fully successful
 - Total number of deployments for this distribution package
 - Description of the distribution package
 - Any additional Notes (if applicable)
- **Origin**
This displays where this distribution package was distributed from.
- **Operating Systems**
This displays operating system platforms that this distribution package can deploy to.
- **Deployments**
The number of deployments previously created for this distribution package.

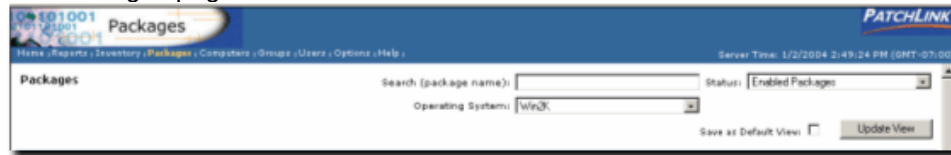
7.2 Page Functions

- Display and Hide

Click the to display additional information and statistics about the represented item. Click the to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (,) is only available for Microsoft Internet Explorer at this time.

- Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Packages page header.



- Search

You may search packages for more granular results by entering the package text into the **Search** field and clicking on the Update View button.

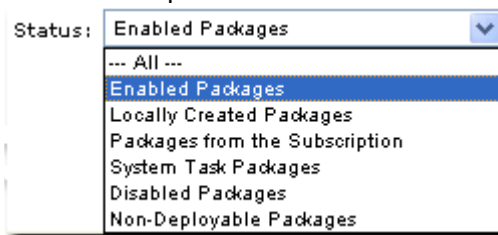
Search (package name):

This will return the package(s) having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

- Status

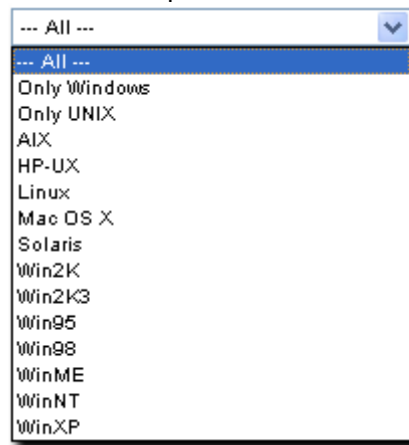
Filter by package status using the dropdown menu and click on the Update View button.



You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

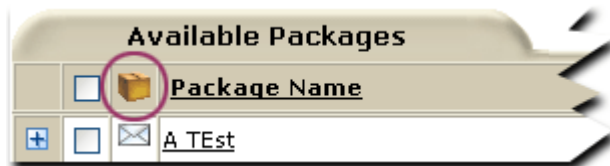
- Operating Systems
Filter by Operating Systems using the dropdown menu and click on the  Update View button.



You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



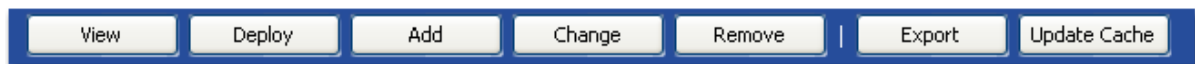
7.3 Package Statuses & Types



New	Current	Tasks	Local	Description
				The package is not cached.
				The package has been scheduled to be cached or is in the process of being cached.
				An error occurred while trying to cache the package.
				The package is cached and ready for deployment.
				The package is currently deploying (animated).
				The package is disabled.

- **New**
This distribution package has been released and its metadata has been downloaded from PLHOST since you began your PLUS session.
- **Current**
This distribution package has been released and its metadata has been downloaded from PLHOST before you began your PLUS session.
- **Tasks**
This is a system task distribution package.
- **Local**
This is a locally created distribution package.
See [Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information on custom packages.

7.4 Action Menu



- **View**
This displays additional information about the distribution package. In this view you can also click to view the distribution package's deployments.
- **Deploy**
This creates a deployment for the selected distribution package. See [Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information.
- **Add**
Create a new local distribution package See [Section 8; Creating and Editing Packages: Package Editor Wizard](#) for more information.
- **Change**
Change a local distribution package. See [Section 8; Creating and Editing Packages: Package Editor Wizard](#) for more information.
- **Remove**
This removes any non-System Task selected distribution packages. PLUS will re-download the package metadata (and not the files or scripts) for any deleted PatchLink provided distribution package (via the PLUS's subscription service). PLUS will only cache the package if it is critical or being requested by a deployment.
- **Export**
Export the distribution package list (and their information) to a comma-separated value (CSV) file. The order of the data is based on what the current display is sorted on.

- **Update Cache**
Initiates the process to cache (or re-cache) for the selected distribution packages. If no distribution packages are selected this will re-cache all of the previously cached distribution packages.

7.5 Distribution Packages Security

*The Distribution Packages section of PLUS requires the **View Packages** access right. If a user does not have the correct access the access denied error message is displayed.*

*To be able to view the deployments for a distribution package requires the **View Deployments** access right. If a user does not have the correct access the hyperlink on the **Package Name** will not be displayed.*

*To be able to create a deployment for a selected distribution package requires the **Deploy packages** access right. If a user does not have the correct access the **Deploy** button is disabled.*

*To be able to create, change or remove distribution packages requires the **Manage Packages** access right. If a user does not have the correct access the **Add**, **Change** and **Remove** buttons are disabled.*

*To export all of the distribution packages and their information to a comma-separated values (CSV) file requires the **Export Package Data** access right. If a user does not have the correct access the **Export** button is disabled.*

*To cache the selected (or re-cache all of the previously cached) distribution packages requires the **Cache Packages** access right. If a user does not have the correct access, the **Update Cache** button is disabled.*

7.6 Deployments

A Deployment, in its simplest form, allows a Patch to be downloaded by a Deployment Agent, so it can install it. In more generic terms, a Deployment is the encompassing instructions around a Distribution Package that describes to the Deployment Agent how to deploy the package. The contents of the Distribution Package contain all the other necessary information (info, files and scripts) required to actually perform whatever needs to be done: install this patch executable, stop this service, validate a system condition, change a database entry, etc.

Deployments can be created throughout the product, but basically encompass three main areas: Vulnerability-based Deployments, Package-based Deployments and a Group's Mandatory Baseline.

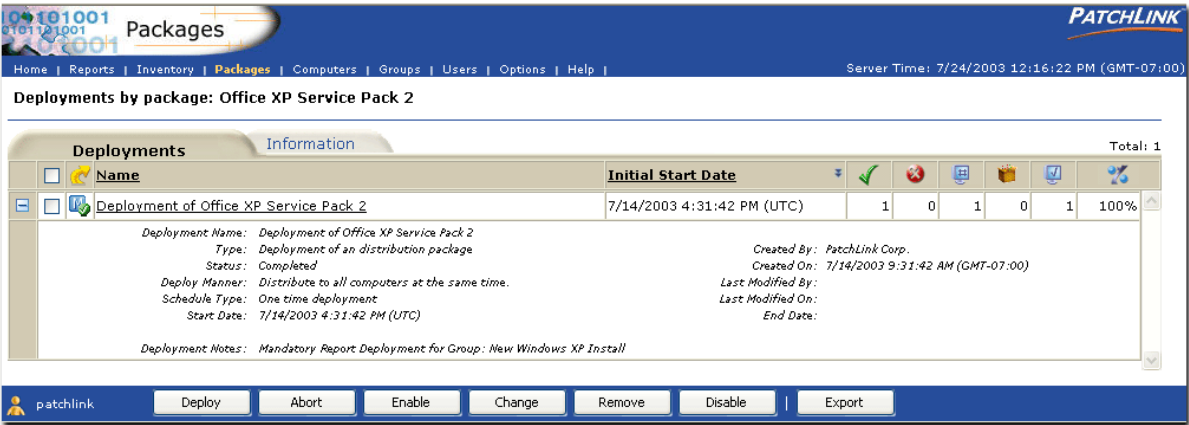
- **Vulnerability-based Deployments**
A Vulnerability contains multiple associated distribution packages and the target package to be deployed depends on the assigned computers. As a computer goes through the Discover Applicable Updates process, it is assigned Vulnerabilities to scan as PLUS determines they are applicable to the computer. Based on these results, a PatchLink User has the ability to determine which computers to deploy the "Patch" (Vulnerability Fix) to. Behind the scenes, PLUS goes through and makes sure that the computers get assigned the correct Distribution Package.

- Package-based Deployments**
 A Distribution Package is assigned a single operating system, thus only those computers whose operating system matches are able to perform the deployment. Package-based Deployments are the easiest to create, though they do not give you the granularity to tell the PatchLink User which computers really apply to this patch (or package) or not.
- Group Mandatory Baseline**
 A group contains a feature called its Mandatory Baseline, or the ability to define a baseline of Vulnerabilities or Locally-created Distribution Packages as being the base set of patches and other packages that must be installed for the group's computer members. In terms of Vulnerabilities, a Mandatory Baseline will continually check to verify and validate that the patch is actually installed; if it is not, it will deploy the necessary distribution package to get it to be installed.

Select a specific **Package Name** link from the Package Name column to view information and deployment details.

The package deployments section displays all of the deployments that have been created for the distribution package.

The Distribution Packages section displays all of the packages that the PLUS has available to it, various functions to manage them, and the number of Deployments created to deploy a package.



Clicking the will display additional information about the deployment. Clicking the will hide this information from view. The information is refreshed each time it is displayed. The deployment information contains:

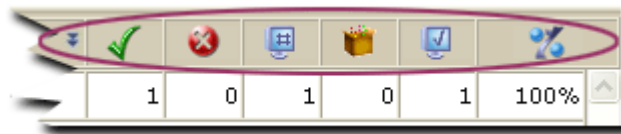
Deployment name	The name of the deployment
Type	Deployment for which type of a package
Status	This can be: - o Enabled - o Disabled - o Paused
Deploy manner	The manner in which this deployment occurred. It can be - o Sequential - o Parallel - o First come first serve - o Distribute to # of computers at a time
Schedule type	This can be: - o Recurring - o One time
Start date	The date and time this deployment was started
Deployment Notes	Additional information about the deployment
Created by	The user who created this deployment
Created on	The date and time this deployment was created
Last modified by	The user who modified this deployment last
Last modified on	The date and time this deployment was last modified
End date	The date and time the deployment was completed

Select a specific **Deployments Package Name** to view deployment details.

- Deployment Types and Status

New	Current	Local	System Task	Mandatory Group	Description
					Deployment with no assigned computers.
					Deployment currently deploying (animated).
					Deployment waiting to start.
					Deployment which all of the assigned computers and groups have finished successfully.
					Deployment in which at least one computer finished unsuccessfully.
					Deployment that is disabled.

- **New:** A new deployment is a deployment that has been created since you logged on to your current session.
 - **Current:** A deployment that was created before you logged on to your current session.
 - **Local:** A deployment is of a locally created distribution package.
 - **System Task:** A system task deployment contains a system task distribution package to perform required or PatchLink provided tasks. These deployments may include automated schedules in which the membership of the deployment may not be modified, though the schedule may.
 - **Mandatory Group:** A deployment is created through the mandatory baseline for a group. This deployment is automatically created and managed through the mandatory baseline process.
- **Name**
The name assigned to the deployment.
 - **Initial Start Date**
The schedule date the deployment is to begin. For recurring deployments this is the first scheduled date of the deployment.
 - **Statistics**



The right-hand side of the vulnerability entry contains columns which illustrates the current result statistics for deployments by package.

Result	Result Definition
	The total number of computers or groups that finished the deployment successfully.
	The total number of computers or groups that finished the deployment unsuccessfully.
	The total number of computers or groups that are assigned the deployment.
	The total number of computers or groups that are in process of executing the deployment.
	The total number of computers or groups that finished the deployment.
	The percentage of the computers or groups that finished the deployment.

7.7 Deployment Summary

This view illustrates the overall information about this particular distribution package including its content, deployment status, etc.

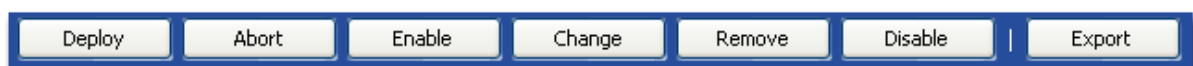
Deployments of a package are designated by the following types:

Result	Result Definition
	Deployment of a mandatory baseline item for a group.
	Deployment of a distribution package (provided by PatchLink).
	Deployment of a new distribution package (provided by PatchLink).
	Deployment of a new distribution package (provided by PatchLink).
	Deployment of a locally-created distribution package.

Each deployment has the following states, depending upon the status results of the deployment (using a distribution package deployment for the deployment type).

Result	Result Definition
	This deployment has not started.
	This deployment is currently in progress. (animated)
	This deployment has finished and all targets of the deployment came back as they deployed the package successfully.
	This deployment has finished and at least one of targets of the deployment came back as it deployed the package unsuccessfully.
	This deployment has been disabled or put on hold.

7.8 Action Menu



- Deploy**
 Deploys the current (selected) package. This will launch the Deployment Wizard. You can quickly schedule a package for deployment or distribution to computers with Client Agents from this wizard. See [Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information.

Note: You will **not** be allowed to create new deployments of System Task Packages from PatchLink (only modify their schedule).

- **Abort**

To abort one or more deployments:

 - Select one or more deployments.
 - Click the Abort button at the bottom of the page.

This will cancel one or more deployments. The computers that have already received the package will not be affected and any other computers will show that the package deployment was aborted before the deployment could occur.

Note: You will **not** be allowed to abort deployments of System Task Packages from PatchLink.
- **Enable**

Click on the Enable button to enable a paused or a disabled deployment. The deployment will then be scheduled to occur according to its schedule type and manner.
- **Change**

This will launch the Deployment Wizard, allowing you to make modifications to any deployment. All deployments can be changed, including deployments of System Task Packages from PatchLink. Note that System Task Packages are automatically assigned to computers, so removing a computer from a deployment of a System Task Package will have no effect (the computer will be re-assigned to the deployment by the PatchLink Update Server). See [Section 8; Creating and Editing Packages: Package Editor Wizard](#) for more information.
- **Remove**

Removes the selected disabled deployments. To remove one or more deployment entries:

 - Select one or more deployments
 - Click the Remove button.

This will delete the selected package deployments from your PatchLink Update Server. Removing a deployment will have no affect on computers that have already received the deployment.

Note: you will not be allowed to remove deployments of System Task Packages from PatchLink.
- **Disable**

Disables the deployment. The deployment will be paused and no longer deployed to the assigned computers.
- **Export**

Export the deployment data to a comma-separated value (CSV) file.

7.9 Deployment Details

The deployment details section displays the assigned computers and groups and the status of the deployment for each. To view the group membership results for the deployment, click on the name of the group, then select that specific deployment package's **Name** link.

Computers and Groups Scheduled for 7/12/2003 1:45:00 PM (Agent Local Time)							Total: 1
☐		Name	Status	Last Run Status	Last Run Start Date	Last Run Completed Date	Next Run Date
☐		\\PDADDY-PC	Completed	Success	7/12/2003 2:48:41 PM	7/12/2003 2:49:54 PM	

- Computer Status



Status	Description
	This is an enabled deployment agent.
	The agent is sleeping as it is outside its hours of operation.
	This is an enabled detection agent that does not correspond to a registered deployment agent.
	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes).
	This agent has been disabled.

- Name
This displays the name of the computer or group. The name of the group is also a hyperlink. Clicking the link will display the members of the group and the status of the deployment for each.

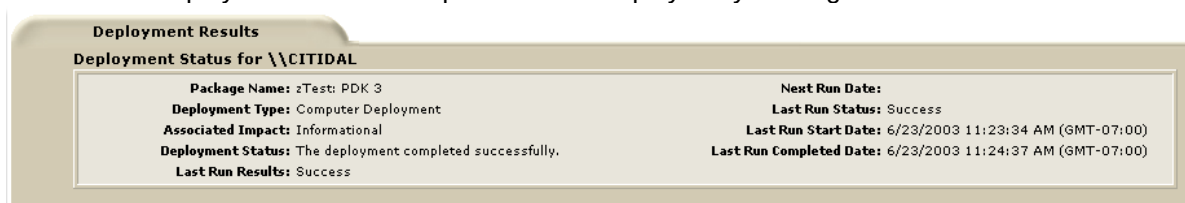
- Status

This displays the status of the deployment for the computer or group.

Status	Description
Not Started	The computer or group has not started the deployment. • The deployment start time has not been reached. • The computer has not contacted PLUS since the start of the deployment. • The deployment or global PLUS deployment limit was full the last time the computer contacted PLUS. It will try again on its next interval.
In Progress	The computer or the group has started the deployment.
Not Running	The computer or group has finished at least the first occurrence of this recurring deployment, but the next instance of this deployment has not started.
Not Scheduled	Computer members of a group are not assigned the deployment for a group deployment until the computer has contacted PLUS once the deployment start time has been reached.
Obtaining Package	PLUS is currently downloading the necessary distribution packages for the deployment. Once they have been cached (and the deployment start time has been reached), the computers will be able to download perform the deployment.
Completed	All computers and groups have finished the deployment.
Disabled	The specific computer or group assignment for this deployment has been disabled.

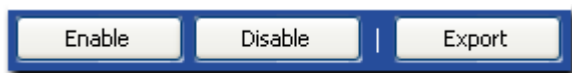
- Last Run Status (link)

This displays the status message from the last time this computer or group performed the deployment. Once the deployment has been performed, the specific results of the deployment for that computer can be displayed by clicking on the status text.



- Package Name: This displays the name of the distribution package that was deployed.
 - Deployment Type: This displays the deployment type.
 - Associated Impact: This displays the impact of the associated vulnerability, if the distribution package is associated to one.
 - Deployment Status: This displays the overall deployment status information.
 - Last Run Results: This displays the results of the last time the computer performed the deployment.
 - Next Run Date: This displays the date when the computer is to perform the deployment again, if the deployment is recurring.
 - Last Run Status: This displays the status of the last time the computer performed the deployment.
 - Last Run Start Date: This displays the date when the computer last started the deployment.
 - Last Run Completed Date: This displays the date when the computer last finished the deployment.
- Last Run Start Date
This displays the date when the computer or group last started the deployment.
 - Last Run Completed Date
This displays the date when the computer or group finished the last deployment.
 - Next Run Date
This displays the date when the computer is to perform the next deployment.

7.10 Action Menu



- Enable
This enables the selected disabled deployment assignments.
- Disable
This disables the selected enabled deployment assignments. Disabled deployment assignments cause the individual deployment for the agent or group to not be performed

while not affecting the overall deployment. Recurring mandatory baseline-based deployment assignments will automatically be disabled after the deployment has failed three times.

- Export

Export the deployment status and details to a comma-separated value (CSV) file. The order of the data is based what the view is sorted on.

7.11 Package Information

Click on the Information tab to display the information about the distribution package. The Information section is broken down into two sections: Package Information and Package Content.



- Package Information

- Name: This displays the name of the distribution package.
- Status: This displays the status of the distribution package.
- Operating Systems: This displays the operating system platforms that this distribution package can deploy to.
- Created By: This displays the user who created the distribution package.
- Created On: This displays when the distribution package was created.
- Last Modified By: This displays the user who last modified the distribution package.
- Last Modified On: This displays when the distribution package was last modified on.

- More Information: This hyperlink will bring up a browser window with a page that displays more information about the distribution package or the vulnerability.
 - License Information: If the distribution package requires a license to be agreed to, then this hyperlink will bring up that license page in a browser window. The license will have to be agreed to before (done when creating a deployment for it) a deployment can be created for the package.
 - Description: This contains additional information about the distribution package or the patch contained inside.
- Package Contents
 - Files: This displays the number of files that are downloaded when the distribution package is deployed.
 - Directories: This displays the number of directories that are created if they do not exist when the distribution package is deployed.
 - Disk Space: This displays the compressed size of the distribution package.
 - Dependencies: This displays the number of other distribution packages, which must be installed prior to this distribution in order to be deployed.
 - Scripts: This displays the scripts that the distribution package contains.

7.12 Action Menu



- Deploy
This creates a new deployment of the distribution package.
- Change
This allows a PatchLink User to change the local deployment package. See [Section 8: Creating and Editing Packages: Package Editor Wizard](#) for more information.
- Wait / Disable / Enable
Wait re-enables the package. Disable the distribution package from being able to be deployed. If the distribution package is already disabled, this button will not be displayed. Enable a distribution package so it can be deployed. If the distribution package is already enabled, this button will not be displayed. This enables the selected disabled deployments so they are now available for computer deployment agents to obtain.
- Export
Export the deployment data to a comma-separated value (CSV) file.

8. Creating and Editing Packages: Package Editor Wizard

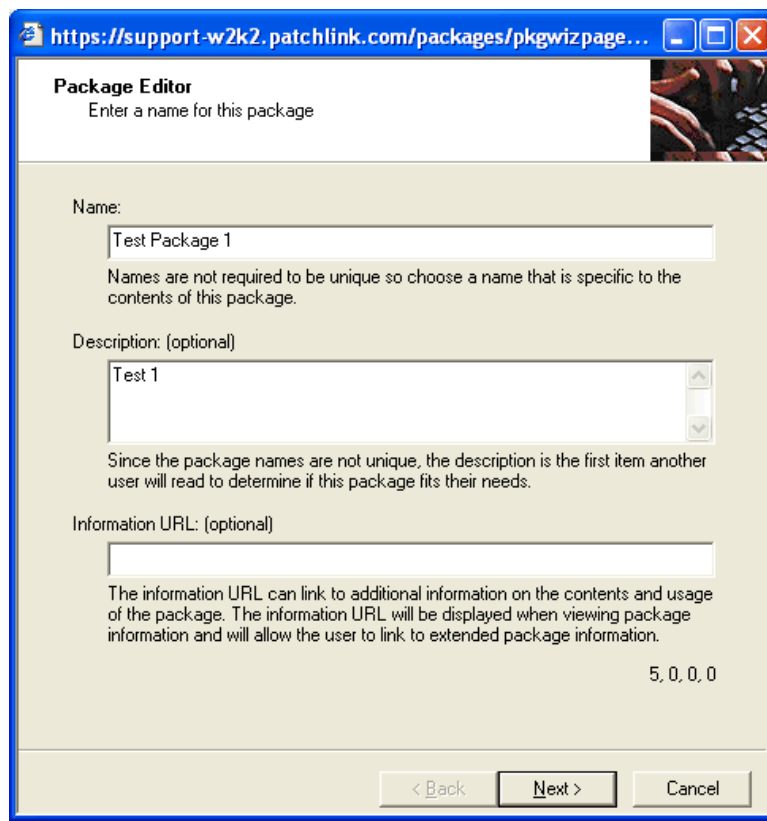
The Package Editor steps through the process of creating or editing packages.

Notes:

- Always test the package within your test network of computers to make sure that there are no unexpected problems before deploying.
- The package editor is an ActiveX control and requires Internet Explorer 5.0 or higher.
- If the Package Editor control has not already been installed on the local browser, it will be downloaded and installed. Once the package editor control has been installed, it will not be downloaded again.

8.1 Create or Edit Package

From the **Packages** homepage, click the **Add** button (or the Edit button if you wish to change a previously created package) on the **Action Menu**. The package editor screen is initialized.



Package Editor
Enter a name for this package

Name:

 Names are not required to be unique so choose a name that is specific to the contents of this package.

Description: (optional)

 Since the package names are not unique, the description is the first item another user will read to determine if this package fits their needs.

Information URL: (optional)

 The information URL can link to additional information on the contents and usage of the package. The information URL will be displayed when viewing package information and will allow the user to link to extended package information.

5, 0, 0, 0

< Back Next > Cancel

- Screen Functions
 - Skip

The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Package Editor Wizard is initialized.
 - Back

The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.
 - Next

The **Next** button initializes the wizard's next screen.
 - Cancel

The **Cancel** button closes the wizard.
- Name:

Enter a name or title for your package. The name is required and you will not be able to move to the next page of the wizard until a name has been entered. Make your package names descriptive but short and remember that two or more packages may have the same name. You may change this name at a later time by modifying this package.
- Description:

An optional description allows you to specify further information about the package. A good practice would be to add additional information as the package is modified, or to provide cautions and/or warnings to the potential user.

 - Deployment Options:

To include a deployment option to indicate a manual installation of the patch is required, please type in (***manual install***) in the description field.

A number of additional deployment options are available here by including them in with the flags delimiter. To add these, add **(PLFlags: flag list goes here)** to the description field.

- y Perform an uninstall (can be used with -m or -q)
- f Force other applications to close at shutdown
- n Do not back up files for uninstall
- z Do not restart the computer when the installation is done
- q Use quiet mode, no user interaction is required
- m Use unattended Setup mode
- l List installed hotfixes
- 1 Force the script to reboot when the installation is done
- 2 The installer may reboot
- yd This option (uninstall) is available on the deployment wizard
- fd This option (Force other applications to close) is available on the deployment wizard
- nd This option (Do not backup) is available on the deployment wizard
- zd This option (do not restart) is available on the deployment wizard
- qd This option (quiet mode) is available on the deployment wizard
- md This option (unattended mode) is available on the deployment wizard
- ld This option (list mode) is available on the deployment wizard
- 1d This option (force reboot) is available on the deployment wizard (and it is controlled by the script)
- PLDO Deploy only, do not run the script just drop the files
- PLNP Do not show a popup to the user

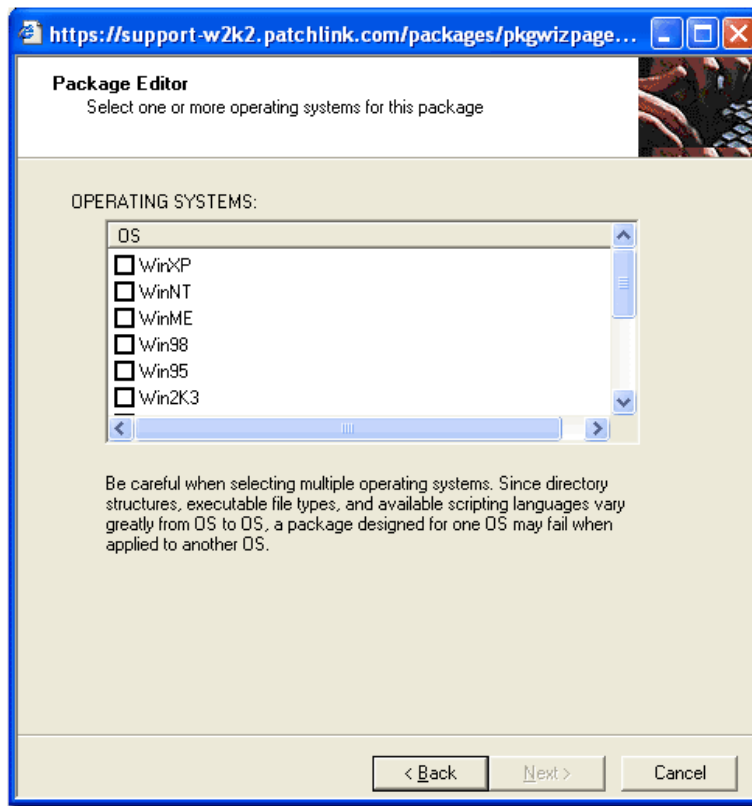
Notes:

- Many setup and installation packages are different and thus, the above flags are likely to change from package to package.
- To add different flags, simply type in their code. There is an input box available in the deployment wizard to allow the user to see the flags not displayed above.
- Information URL
The optional information URL can link to additional information on the contents and usage of the package. The information URL will be displayed when viewing package information and will allow the user to link to extended package information.

Click on the **Next** button to initialize [the](#) wizard's next screen, which allows you to select operating systems

8.2 Operating Systems

The Operating Systems screen allows you to select which Operating Systems you wish to deploy the package to.



To select an Operating System, click in the checkbox to the left of the Operating System name. You can not click on the **Next** button until you have chosen at least one Operating System.

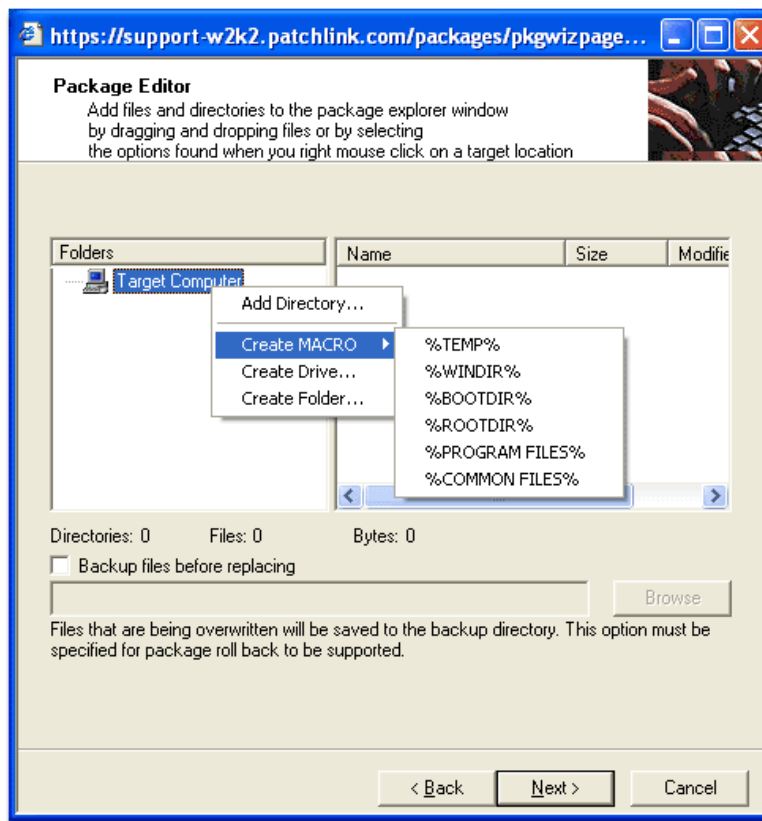
Note:

Be careful when selecting multiple Operating Systems. Since directory structures, executable file types, and available scripting languages vary greatly from Operating System to Operating System, a package designed for one Operating System may fail when applied to another Operating System.

After you have selected the operating system(s) you wish to deploy to, click the **Next** button.

8.3 Adding Files

The File Editor screen allows you to add files to the package and describe where the files will be installed when the package is deployed to the computers on your network.



A Windows Explorer type window initializes with a directory tree on the left starting at "Target Computer" and a file list on the right. Initially, these are both empty except for the "Target Computer" in the tree view. The Target Computer folder signifies the computer(s) on which this package will be installed. It is automatically created for you and cannot be deleted.

You can begin to add files and/or directories to the package by either:

- Right-Mouse clicking on the "Target Computer" and selecting one of the options from the popup menu.
- Drag directories from a Windows Explorer or My Computer window onto the Target Computer.
- You can also drag files from a Windows Explorer or My Computer window onto any drive or directory in the tree view or into the file list.

Note:

We recommend using the temp directory when delivering the package to your target computer. The files will be deployed to %systemroot%\temp directory (c:\winnt\temp on Windows 2000 Computers).

Once the files you want in the package have been added, or while you are adding them, you can create the directory structure for the package. You can right mouse click on most of the items in either window for options on adding, renaming, or deleting items. You can also drag and drop items from one place on the tree to another or from one window to another in much the same way you would in Windows Explorer. The Right-Mouse Click options are:

- **Add Directory**

This option will bring up a file system browse window, where you can select which directory you wish to add. This option is always available.

- **Add Files**

This option will bring up a file system browser window, where you can select which files you wish to add. This option only becomes available once there is a directory level created (or added) under Target Computer.

- **Create MACRO**

You may create Folders from what are referred to as Macros. Any macro name can be created by placing matching % sign's around a word when using the **Create Folder** option. The file editor allows you to create common macros by using the **Create Macro** option when right-mouse clicking on the Target Computer. Macros can be environment variables that are defined in the System Environment or special macros that only the Client Agent can expand. The following are a few examples of common macros:

%TEMP%	The <i>operating system</i> temp directory location. %TEMP% is a macro that is guaranteed to exist on most systems. If it's not found in the <i>operating system</i> environment then it is created. %TEMP% typically expands to c:\Windows\Temp, c:\Temp, c:\WinNT\Temp, or /tmp depending on <i>operating system</i> and configuration.
%WINDIR%	The <i>operating system</i> windows directory location. %WINDIR% typically expands to c:\Windows.
%BOOTDIR%	The <i>operating system</i> boot directory location. %BOOTDIR% typically expands to c:\.
%ROOTDIR%	The <i>operating system</i> root directory location. %ROOTDIR% typically expands to c:\.
%PROGRAM FILES%	The <i>operating system</i> program files location. %PROGRAM FILES% typically expands to c:\Program Files.
%COMMON FILES%	The <i>operating system</i> common files location. %COMMON FILES% typically expands to c:\Program Files\Common Files.

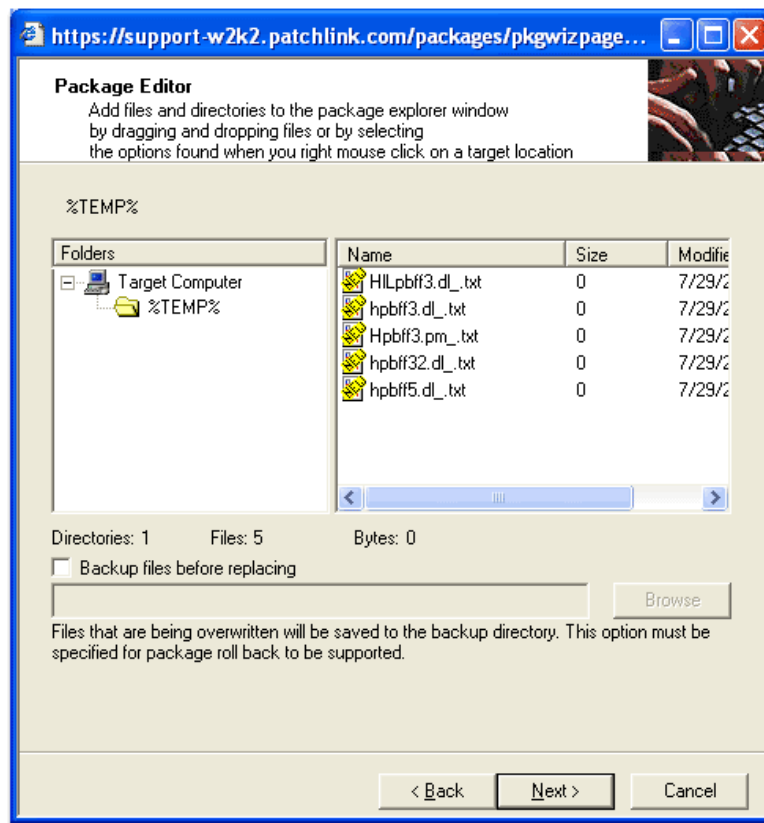
Not all macros are available on all *Operating Systems*. Please only choose the macros that are available for the operating systems and configurations you are using. This option only becomes available on the directory level directly under *Target Computer*.

- **Create Drive**

If your standard computer installation uses drives other C:\ or this package will be deployed to computers that use drives other than C:\, you can add drives to the package by right mouse clicking on the Target Computer and selecting the Create Drive option. Once the drive is created you can drag and drop the files or folders as needed to create the correct directory structure.

- **Create Folder**
This option brings up an input window. This window allows you to type in the directory name you wish to create. This option is always available.
- **Delete**
This option will delete the directory or file you have right-mouse clicked on. This option is only available on directories or files under the Target Computer.
- **Rename**
This option will rename the directory or file you have right-mouse clicked on. This option is only available on directories or files under the Target Computer.

You may place files in any Drive, Folder, or Macro Folder you create. You can rename any file or folder. The package editor will keep track of where the original files were found. No changes will be made to the path names or file names on the computer on which the package editor is running as you are building a representation of where the files will be installed when the package is deployed.



Note:

Please delete all directories that you do not want installed when the package is deployed as the empty directories will be created on the target computer.

- Backup Directory

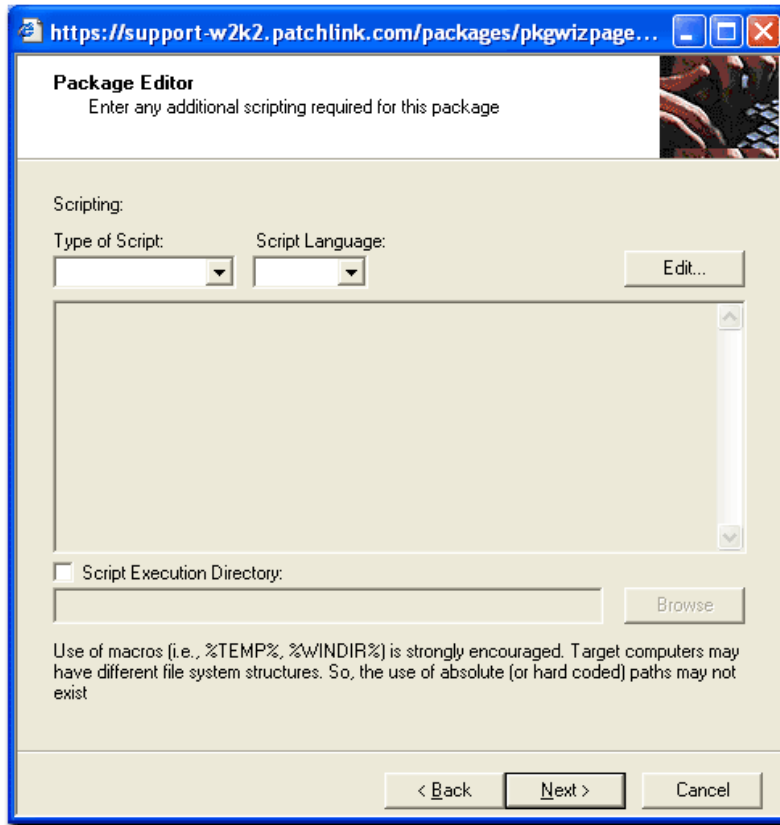
Select "Backup files before replacing" if you wish to create a backup of the files that you are adding to the package. With a backup enabled, when the agent downloads a file it will check to see if the file already exists on the machine. If it does exist the agent will first copy the original file to the backup location then replace the file with the new version from the package. Enter the backup directory path in the text box below the option or use the *Browse* button to search for the path.

Click on the **Next** button to initialize [the](#) wizard's next screen, which allows you to create scripts to run at deployment time

8.4 Create Scripts

The Create Scripts screen allows you to create scripts that will be run on the computer during the deployment process. A software package can have up to three scripts, one of each type. Scripts are executed in the follow sequence:

- Pre-Script
- Files are downloaded and copied to target locations
- Command Line Script
- Post-Script



The screenshot shows a web browser window with the address bar displaying <https://support-w2k2.patchlink.com/packages/pkgwizpage...>. The main content area is titled "Package Editor" with the subtitle "Enter any additional scripting required for this package". Below this, the "Scripting:" section contains two dropdown menus: "Type of Script:" and "Script Language:". To the right of these menus is an "Edit..." button. Below the dropdowns is a large text area for entering script content. At the bottom of the scripting section, there is a checkbox labeled "Script Execution Directory:" followed by a text input field and a "Browse" button. A note at the bottom of the window states: "Use of macros (i.e., %TEMP%, %WINDIR%) is strongly encouraged. Target computers may have different file system structures. So, the use of absolute (or hard coded) paths may not exist". At the very bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

- Script Types
 - Pre-Script

The Pre-Script can be used to test for a condition of the machine, shutdown a service, etc. For example; you can stop the package rollout in the pre-script by using the SetReturnCode in the PLCCAgent script object. Pre-Scripts can take the form of VBScript or JScript.
 - Command Line

Command Line Scripts are often used to launch executables. The format is the same as a standard CMD or BAT file.
 - Post-Script

Post-Script can be used for any clean-up operations, delete files, start services, run a installer, etc. Post-Scripts can take the form of VBScript or JScript.
- Script Editor
 - Script Type

Select the type of script you would like to execute from the Type of Script dropdown box.
 - Script Language

Select scripting type from the Script Language dropdown box.
 - Script Execution Directory

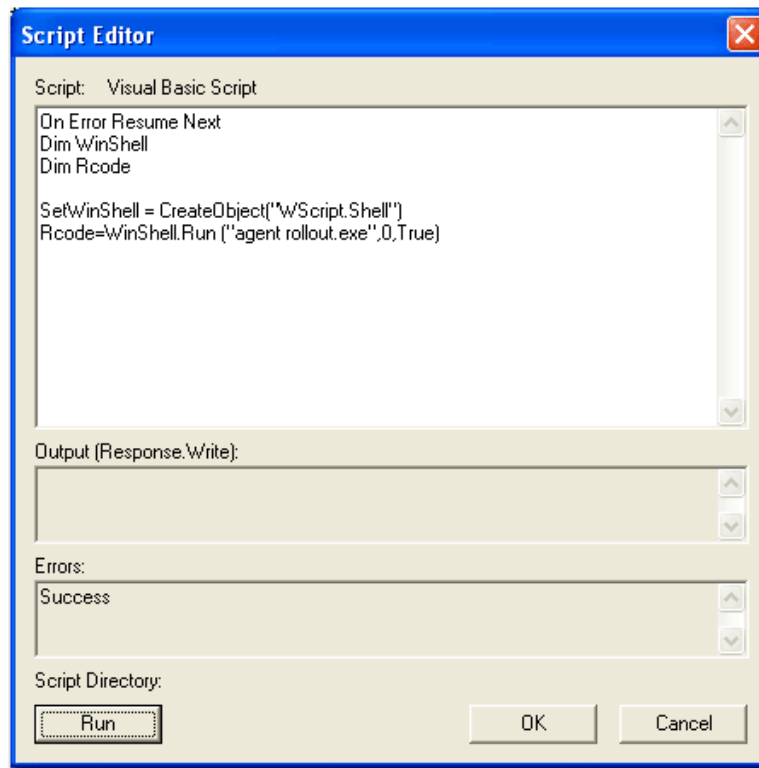
Select Script Execution Directory if you want your script to run somewhere other than the default location. Enter the backup directory path in the text box below the option or use the **Browse** button to search for the path.
 - Edit Script

Click the **Edit** button. This will display the Script Editor dialog.

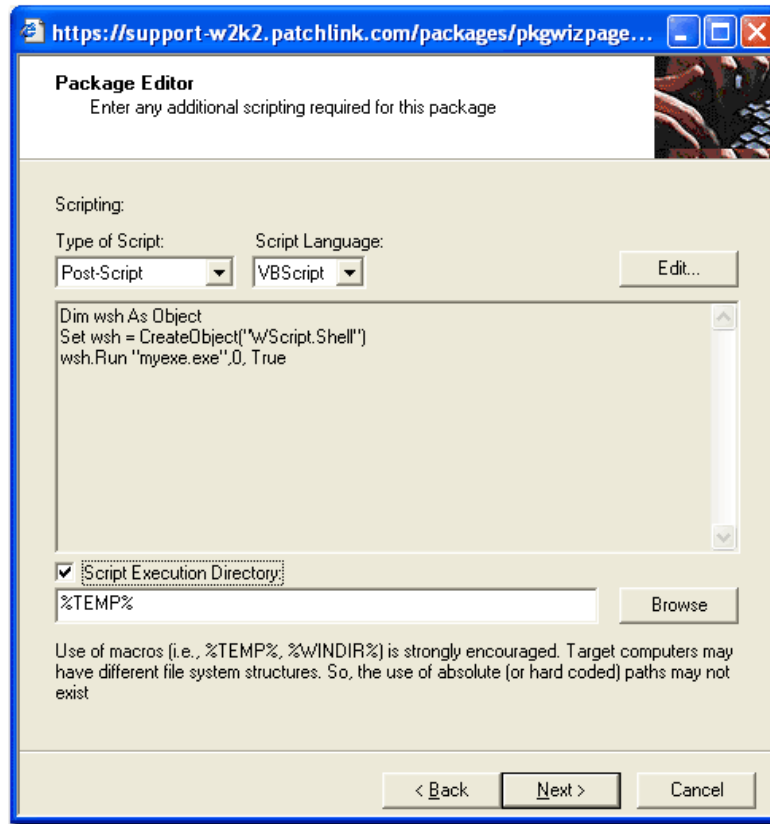
Note:
We recommend using a VB Script to tell the agent what to do with the package.

Click the **Edit** Button to create your script.

Here is a simple VB Script below that will just execute the package once the package gets delivered to the target computer.



Test the script by click the **Run** button on the bottom left corner. View the **Errors** field: If the results read "success," click the **OK** button to close his window and the **Next** button to initialize the next window. If you get a failure message, correct your script until a success message is achieved.



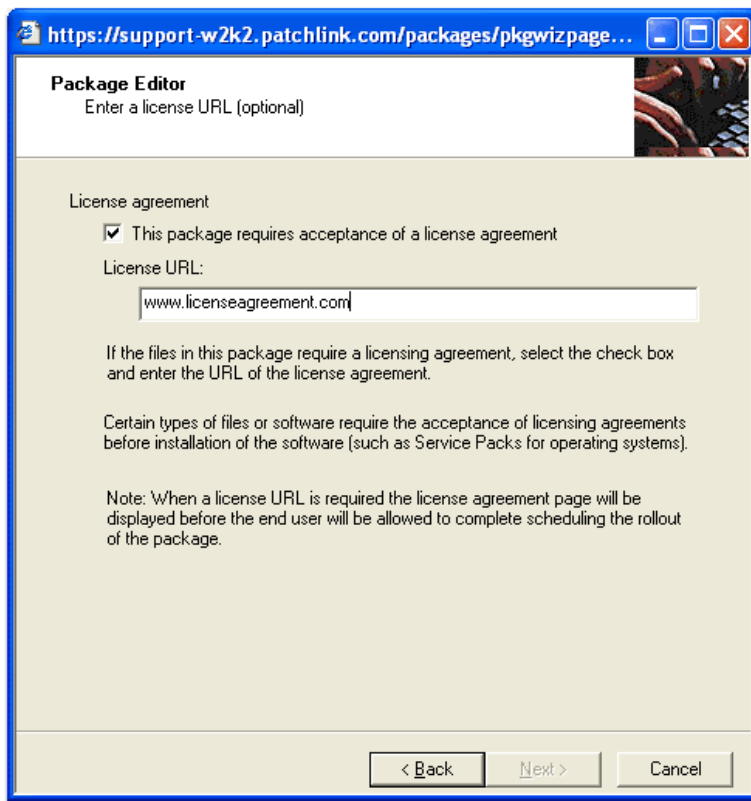
Click the Next button to initialize [the](#) wizard's next screen, which allows you to select package dependencies.

8.5 License URL

The License Agreement screen allows you to enter in an optional License URL, which can link to licensing information for the contents of the package.

This is not normally used for packages that are in-house file distributions. It is primarily for packages containing items such as operating system service packs, device drivers, etc. The License URL will be displayed when viewing package information and will allow the user to link to the license information.

Simply select the License Agreement checkbox and type in the URL destination address of the License Agreement.



The screenshot shows a web browser window with the address bar displaying `https://support-w2k2.patchlink.com/packages/pkgwizpage...`. The main content area is titled "Package Editor" and contains the following elements:

- A header section with the text "Enter a license URL (optional)".
- A "License agreement" section with a checked checkbox labeled "This package requires acceptance of a license agreement".
- A "License URL:" label followed by a text input field containing the value `www.licenseagreement.com`.
- Explanatory text: "If the files in this package require a licensing agreement, select the check box and enter the URL of the license agreement."
- Additional text: "Certain types of files or software require the acceptance of licensing agreements before installation of the software (such as Service Packs for operating systems)."
- A "Note:" section stating: "When a license URL is required the license agreement page will be displayed before the end user will be allowed to complete scheduling the rollout of the package."
- Navigation buttons at the bottom: "< Back", "Next >", and "Cancel".

When scheduling a deployment of the package, the license page will be displayed, and the end user will be required to click the Accept button to complete scheduling the deployment.

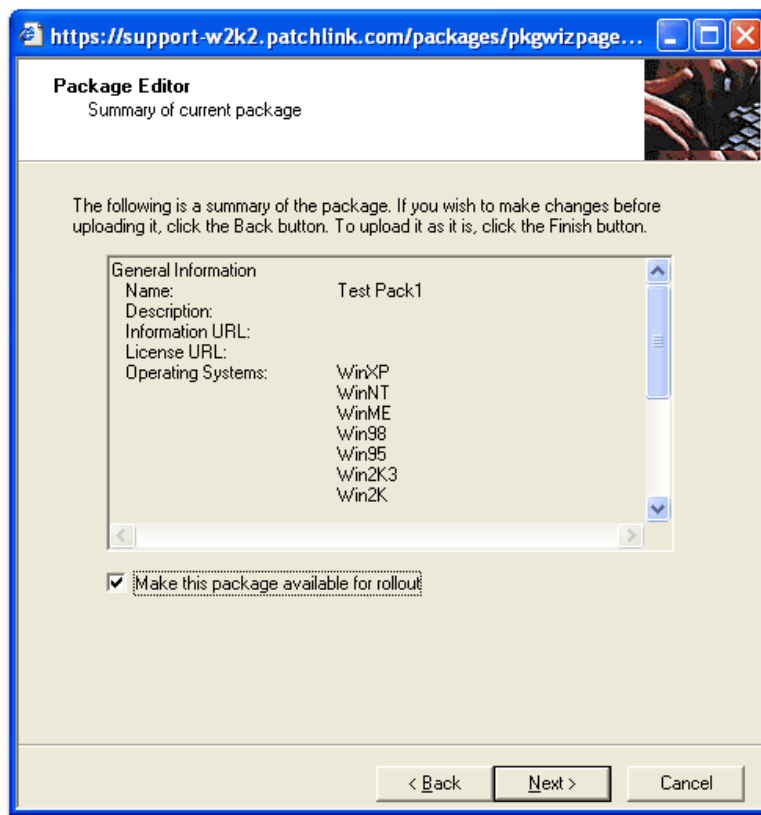
After entering the License URL (optional), click the Next button to initialize [the](#) wizard's next screen, which is a summary of the package.

Note:

If you select the License Agreement checkbox, you must type in the URL destination address of the License Agreement to initialize the **Next** button.

8.6 Summary

The Summary screen displays a simple summary of the package before the package created or the changes are committed.

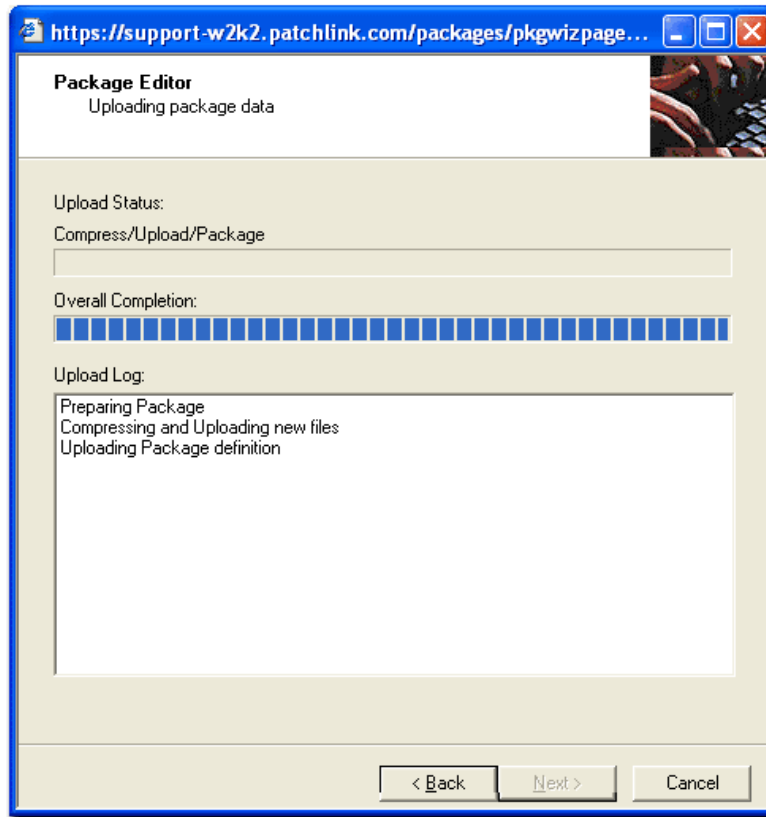


Selecting the **Make this package available for rollout** checkbox, will enable the package to show up in the list of available packages / available for deployment (once the package is created). You may wish to de-select this item if you are creating a skeleton package that will have additional files or details added at a later date or do not wish to have the package scheduled for deployment at this time.

Click the **Next** button to initialize the wizard's next screen, which will commit the changes, create the package, and upload the package data.

8.7 Upload

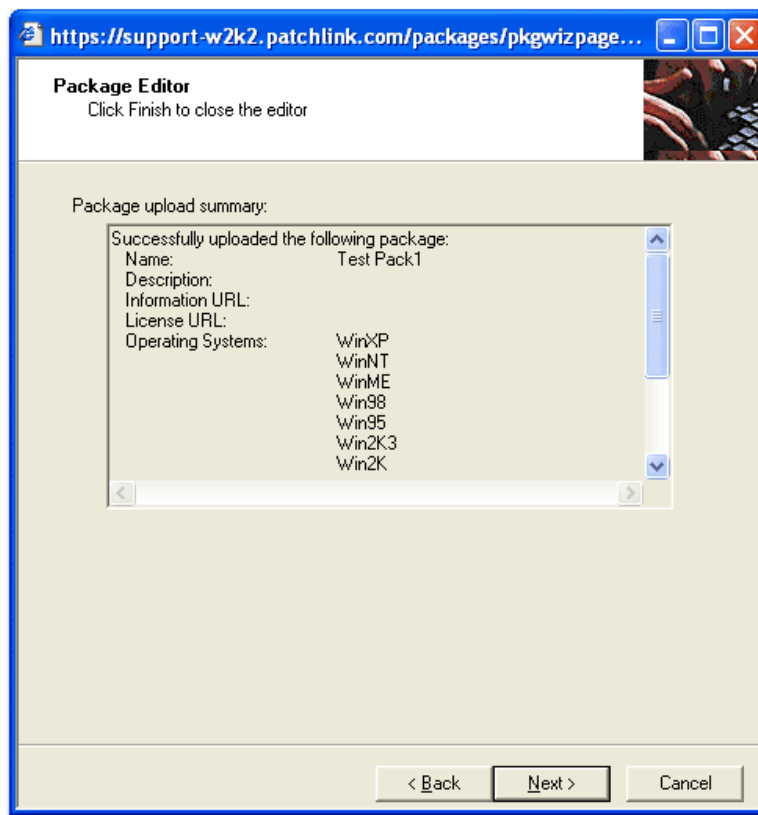
The Upload screen appears verifying that the data is unpacking and uploading.



Once the Upload is complete, the **Next** button will initialize. Click the **Next** button to initialize the Updated Summary screen.

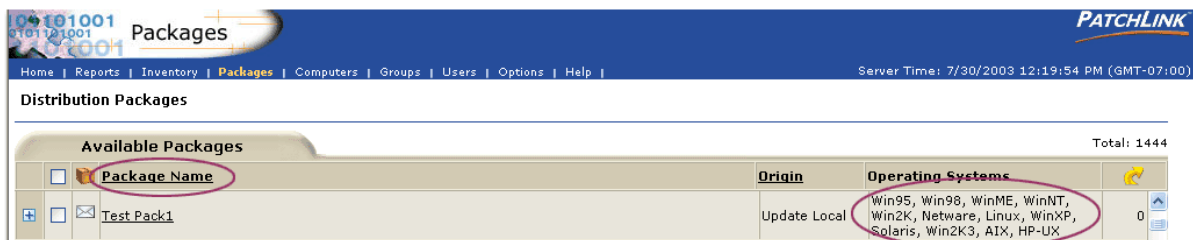
8.8 Updated Summary

The final screen displays a simple summary on the saving of the package, and whether it was successful or failed. If a failure occurred, the error code and description will be displayed.



Click the **Finish** button to close the wizard and complete the operation.

Upon refreshing of the **Packages** page, you can view your package by the name you gave it upon creating it, and view the operating systems that you chose to deploy to during the patch building process.



9. Deploying Packages: Schedule Deployment Wizard

Use this section in congruence with [Section 7; Packages](#), as Section 8 describes the intricacies of packages, deployments, events and statistics, while Section 9 focuses on the physicality of the actual package deployment.

After the PLUS is installed and agents are deployed, it is necessary to conduct some analysis of the vulnerabilities present within the computers on your network.

When conducting initial remediation, it is wise to begin with service packs and cumulative patches first, as this will significantly decrease the number of individual patches that need deployment.

Once the necessary computers are fully patched, it will only be necessary to deploy the new patches that are made available each week.

Let us first understand the PatchLink Update Deployment Logic: Q-Chain and Standard Deployments

Q-Chain

Q-Chain allows you to deploy multiple packages (providing they are Q-Chainable) with only one reboot. It correctly orders the installed files so the most recent version of each file is applied.

A Q-Chainable Package is a package that gives you the option to deploy it as a Q-Chain.

A Q-Chain Deployment is a Q-Chainable Package that is deployed as a Q-Chain. (A Q-Chainable Package that is not deployed as a Q-Chain is NOT a Q-Chain Deployment). The PatchLink Update Agent runs the local copy of qchain.exe after each Q-Chain Deployment.

Standard Deployment

For the purposes of this document, a **Standard Deployment** is either a non-Q-Chain Deployment or a Q-Chainable Package that is not deployed as a Q-Chain Deployment.

Reboot Deployment

There are two Reboot deployments.

Reboot is a System Task package found on both the Packages page and the Computer Deployments page. This reboot occurs following any deployment requiring a reboot in which the reboot is not suppressed (this includes Q-Chain deployments) or when the PLUS administrator selects Reboot Now in the Computers page of the PLUS Web interface.

Task – Reboot System is a Vulnerability Report which schedules a reboot at a specified time based on the information entered in the Deployment Wizard.

Dirty State

A PatchLink Update Agent that is in a “clean” state is represented on the Computers page of the PatchLink Update Server Web interface by icons that do not contain a “C” or “R”, while the presence of a “C” or “R” denotes a “dirty” state.

The **dirty state “C”** indicates that the agent received a Q-Chain deployment in which the reboot was suppressed. While in the “C” state, the agent will only deploy another Q-Chain deployment or one of the Reboot deployments, and either type of deployment or a manual reboot will clear the dirty state.

The **dirty state “R”** indicates that the computer received a standard deployment requiring a reboot, yet the reboot was suppressed. This can include either a standard, non-Q-Chain, deployment or a Q-Chainable Package that *was not* deployed as a Q-Chain but NOT a Q-Chainable Package that was deployed as a Q-Chain (in the latter case, the state of the agent would be “C”). While in the “R” state, the agent will only deploy one of the Reboot deployments, and either type of Reboot deployment or a manual reboot will clear the dirty state.

The following logic is derived from the information above:

1. An Agent cannot go directly from the “R” state to the “C” state.
2. An Agent cannot go directly from the “C” state to the “R” state.
3. Once the Agent goes into either the “C” or “R” state, it will remain in the dirty state until it reboots.

PatchLink Update Deployment Logic

When deploying more than one patch to an individual computer or to a group, the patches can be ordered by scheduling each deployment at a different time, at least one minute apart. In addition to scheduled time, however, the deployment order is also based on deployment type (Q-Chain, standard/non-Q-Chain, Reboot, etc.) and state of the agent (clean vs. dirty).

Deployments proceed in the following order unless the agent enters a dirty state:

1. Q-Chain deployments
2. Standard (non-Q-Chain) deployments
3. System Task: Reboot
4. Task – Reboot System
5. Discover Applicable Updates (DAU) and Refresh Inventory Data (RID)

Within each group (or deployment type), deployments are ordered by their scheduled time. Although no deployment will occur *before* its scheduled time has elapsed, a Q-Chain deployment whose time has elapsed will always precede a Standard deployment whose time has also elapsed.

Once an agent enters a dirty state, only specific deployments can occur, as discussed in the Dirty States section above. In the dirty state “R”, a Reboot deployment will precede both Q-Chain and Standard deployments. In the dirty state “C”, a Reboot deployment precedes any Standard deployments. Once the agent returns to a clean state (i.e. following a manual reboot or a Reboot deployment), deployment again proceeds in the order stated above.

If multiple Q-Chain deployments are scheduled and some have the final reboot suppressed and some do not, the determination of whether a final reboot occurs is based on the last scheduled deployment.

Mandatory Baselines

Although deployments that are part of a Mandatory Baseline cannot be ordered because their scheduled times cannot be controlled, Q-Chain deployments still precede non-Q-Chain deployments.

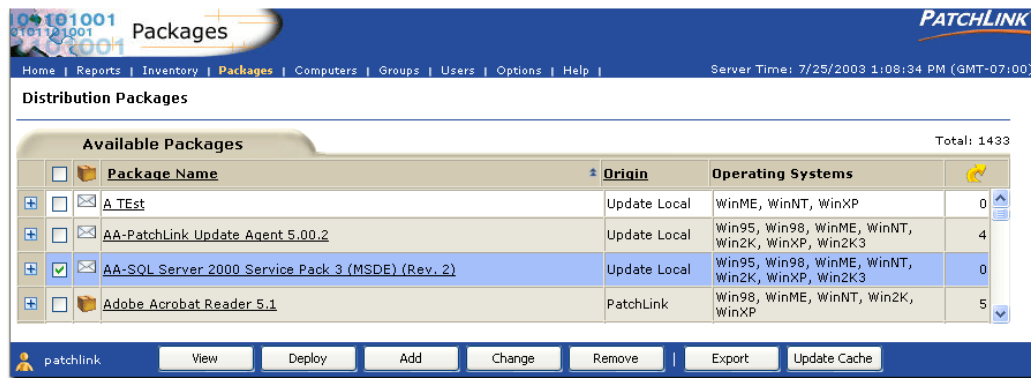
The “Use Q-Chain” and “w/o reboot” options in the Group Mandatory Baseline setup apply only to Q-Chainable packages in the baseline.

The Deployment Wizard steps through the process of selecting computers that will receive that package, select a one time or recurring deployment, and select the date and time to deploy the package.

Note:

Always test the package within your test network of computers to make sure that there are no unexpected problems before deploying.

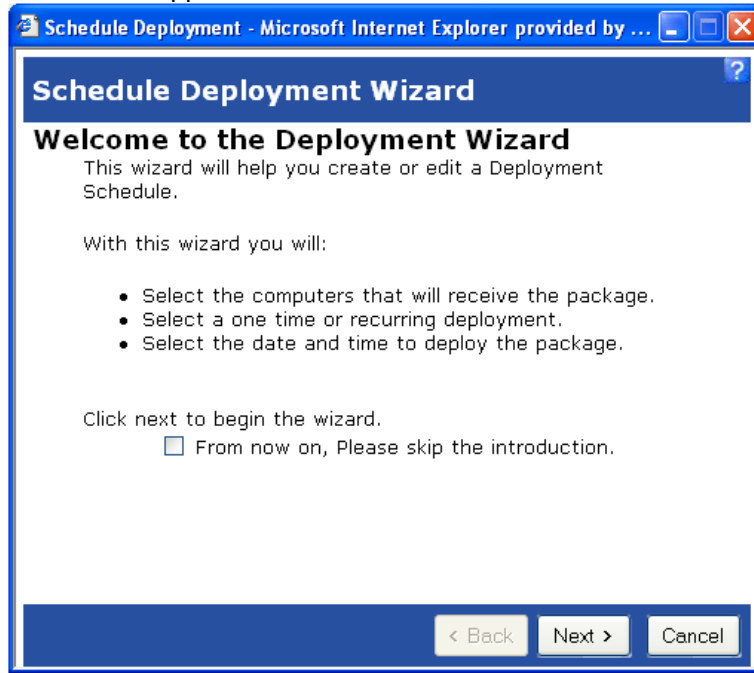
Select the patch you wish to deploy by clicking on the bulletin hyperlink.



From the list of computers that require this patch, click the checkbox next to the item to select, and click on the **Deploy** button to launch the **Schedule Deployment Wizard**

9.1 Welcome

The welcome screen appears.



- Screen Functions
 - Skip

The Skip the Introduction checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Schedule Deployment Wizard is initialized.
 - Back

The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.
 - Next

The **Next** button Initializes the wizard's next screen; the package selection page. This screen will appear if you have not previously selected something to deploy. If you have selected a vulnerability or package, then the next button will take you directly the next screen; the individual computer and computer group selection page.
 - Cancel

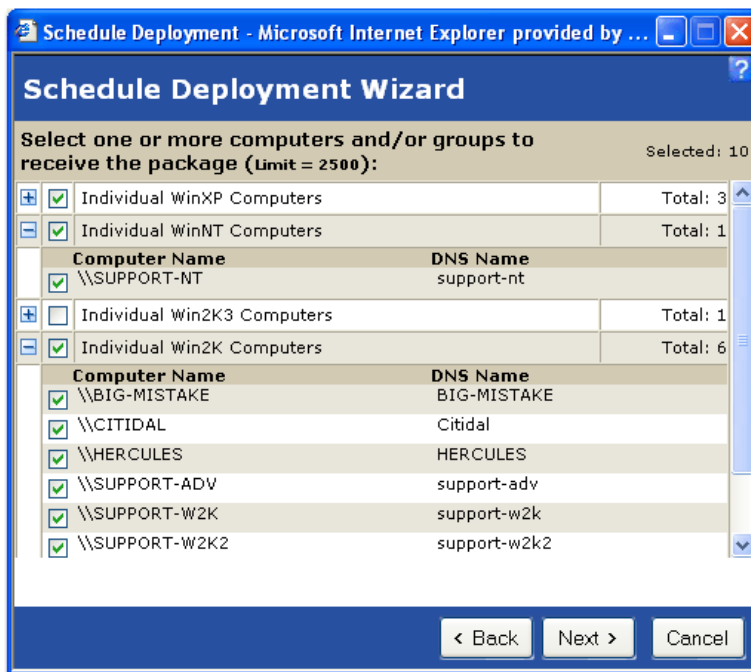
The **Cancel** button closes the wizard.

Click the **Next** button to initialize the **Package Selection** screen.

9.2 Package Deployment Target Selection Actions

This screen displays a list of all individual computers and computer groups that you can deploy to based upon:

- The operating system supported by the package or vulnerability being deployed.
- The agents which the vulnerability applies to (only if deploying a vulnerability).



In addition to the individual computers and system-created computer groups, there is a list of all the user created computer groups present on the PatchLink Update Server. For system and user based group deployments, the determination of which member computers get the deployment is only determined at the start of the deployment.

Initially, the operating systems, the system groups and the user groups are displayed along with the total number of client agents associated with each of them.

To select all computers of a given operating system, click in the checkbox next to each operating system category. (Limit = 2500)

Click the to display and select additional or individual computers within a group. All of the computers for that category will be displayed by computer name and DNS name. Hovering the mouse over the computer name will display the description and hovering over the DNS name will display the IP address. If there is no DNS name provided, the IP address will be displayed.

A deployment requires that at least one computer is selected. The wizard will not advance to the next step until at least one computer is selected. If the wizard is being used to deploy a package associated with a vulnerability, then the computers that were selected from the Vulnerabilities page will be selected automatically.

At the top right corner of the wizard, the total number of selected computers will be displayed.

If launching the deployment wizard from the Vulnerabilities page when the vulnerability does not have a package associated with it, it will be possible to select a package or packages that do not cover all of the operating systems of the computers. In this case, only the computers that match the operating systems of the package will be added to the deployment.

Notes:

This screen does not show up if you have previously selected the package or vulnerability to deploy.

Selecting the checkbox selects all computers in the group.

Click on the **Next** button to initialize the **Deployment Schedule** screen.

9.3 Deployment Schedule

The Deployment Schedule screen contains scheduling information.

Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Select schedule type:

☒ One time On: 7/25/2003 At: 2:01 PM

☐ Recurring

< Back Next > Cancel

Schedules can be one of the two types:

- One Time: (Default)

A one time schedule will start deployments on the selected day at the selected time. If a one time deployment is scheduled for a date and time in the past, then the computers will start the deployment the next time they contact the PatchLink Update Server.

Note: a Select schedule type of **At Registration** appears at the initial deployment of Packages screen. This allows you to deploy the packages upon them registering to a PatchLink Server. An **At Registration** task is only valid for System Packages and will run when a client agent registers at the server. The **At Registration** option is only shown for System Package distributions.

Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Select schedule type:

☒ One time On: 7/25/2003 At: 2 : 01 PM

☐ Recurring

< Back Next > Cancel

Calendar - Microsoft In...

August 2003

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

OK Cancel

Click on the Calendar Launch Button  to initialize the calendar and set the desired date. Click on the hour, minute, and AM/PM drop down menus to select the desired time.

- Recurring

A recurring task will start on the given start date and will occur at the given interval and will stop if a stop day is specified. Click on the radio button to initialize the recurring task window.

Recurring deployments can be scheduled to occur either:

- Daily
- Weekly (You can choose the days in a week when you want the task to recur.)
- Monthly You can choose from a day number in a month (first day in the month's chosen) or a day in a week of every month (first Monday in the month's chosen)

Each of these can also be scheduled to occur at a specific time during the day or recurring several times during the day at a given interval and between certain hours. Finally each of these can be scheduled to end on a given day or continue with no ending date.

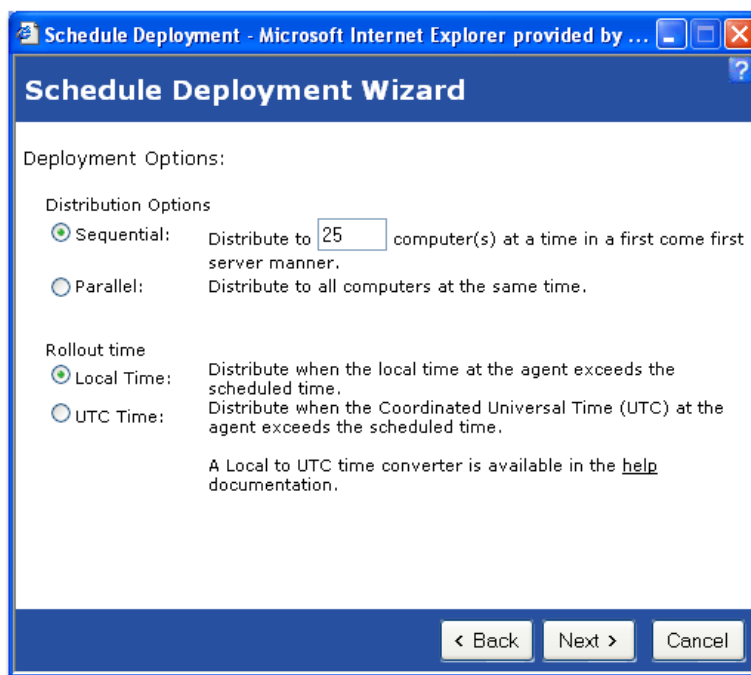
- At Registration

An "at registration" task is only valid for System Packages and will run when a client agent registers at the server. The "at registration" option is only shown for System Package distributions.

After you have made or modified your schedule selections, click the **Next** button to initialize the **Deployment Options** screen.

9.4 Deployment Options

A deployment has two very distinct sets of options to define how the deployment is going to behave. These sets of options are: Distribution and Rollout Time.



- Distribution Options
 - Sequential

Only deploy to a maximum number computers at a time, on a first-come first-serve basis. The maximum limit is configurable for all deployments and is defaulted to 25 computers. If a computer takes longer than an hour to complete the deployment, it is no longer counted against the limit (example: the computer may have been turned off). As computers finish the deployment other computers will begin to receive the deployment, as long as the maximum number is not exceeded.

A sequential deployment will both limit the bandwidth required from the server and infrastructure, as well as halt the deployment should an error occur to a bad patch or other deployment problem.
 - Parallel

Deploy to all computers as they communicate with PLUS to get their next deployment

Use the parallel option if bandwidth is not a consideration, and automatic halt features are not required.

- Rollout Time Options

A deployment will only be given to a computer when the computer's given time has exceeded the start time of the deployment.

- Local Time

Local time will vary depending on the time zone of your location (daylight savings time may apply). When the computer communicates with PLUS, the local time of the computer is checked to see if there are any deployments available. If you have three computers (each in their own time zone) that communicate with PLUS at the same time, each start the deployment when their local time has exceeded the start time of the deployment. Simply put, they will each start the deployment at different times with respect to PLUS.

- UTC Time

Coordinated Universal Time (UTC), is a standardized measurement of time that does not depend on your local time zone. The time in one geographical location is exactly the same time in another. UTC is also known as World Time, Z Time, or Zulu Time. When the computer communicates with PLUS, the UTC time of the computer is checked to see if there are any deployments available. If you have three computers (each in their own time zone) that contacted PLUS at the same time, each will start when the UTC time has exceeded the start time of the deployment. Simply put, they will each start the deployment at the same time with respect to PLUS.

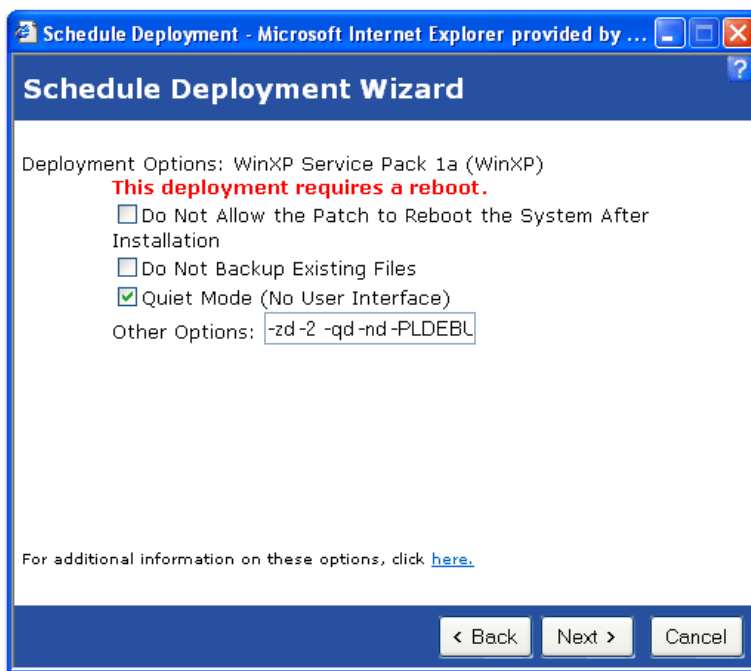
Notes:

- The start time for both of these deployment types depend on the time given by the computer; so the accuracy of the computer's internal clock is important. Hence, when a computer's internal clock is slow, fast or incorrectly set, the scheduled start time of the deployment for that computer is affected.
 - Deployments created to a group will always default the time to UTC since the determination of which members of the group get the deployment is not calculated until the start of the deployment.

After you have made your option selections, click the **Next** button to initialize the next **Deployment Options** screen.

9.5 Deployment Flags

Deployment options include options related specifically to the installation process during the deployment. The deployment comes pre-configured with these options to optimize the deployment's performance. These options are selected based on the behavior of the package's installer program and previous testing by PatchLink personnel. If more than one deployment package is available for deployment, then there will be multiple screens that you must go through to verify these options. These deployment options are placed in to a variable used by the deployment's post script.



- Hotfix Setup Programs

See [Microsoft Windows 2000 Hotfix Installation and Deployment Guide](#) for additional information on Microsoft specific command-line parameters for Hotfix Setup Programs. These options are:

- **This deployment requires a reboot.**

This item shows up only if the package which is being installed may require a reboot of the operating system in order to finish the deployment. This reboot function is not controlled by the deployment script, but can be turned off by selecting the **Do Not Reboot** checkbox

- Uninstall (When available from vendor)

This option will tell the package's installer to uninstall the package from the selected computers.

Note:

If multiple packages replace the same file and you want to successfully return your system to its original state, you must remove the most recently installed package first.

- Force Applications Close

This option will tell the package's installer to force all applications to close when the computer is in the shutdown process.

- **Force a Reboot**

This option will tell the deployment script that a reboot *must* be performed before this deployment is complete.

Notes:

- The script is controlling the reboot in this situation and a reboot will occur regardless if the installer requires it or not.
- This option can not be selected if the Do Not Reboot option is checked.

- **Do Not Reboot**

This option will tell the package's installer to not reboot once the package is installed on to the computer. If the notice that the deployment requires a reboot is shown it is recommended that you do not select this option. If this option is selected anyway, do NOT install any additional programs until a reboot happens. Do not expect the package to be available until a reboot occurs, since many installations require a reboot to finish the installation process.

Note:

This option can not be selected if the **Force a Reboot** option is checked

- **Do Not Backup Existing Files**

This option will tell the package's installer to not backup the existing files. These files are used by the uninstaller. Do not select this option if you wish to uninstall the package at a later time.

The installer controls this action and should not be confused with the deployment backup option, which will only back up the deployment package (not the installed files from the package).

- **Quiet Mode (No User Interface)**

This option will tell the package's installer to function in quiet mode. This mode will not produce any user interfaces (in case any user is logged on to the computer at the deployment time) or require user interaction during the deployment process.

- **Unattended Setup Mode**

This option will tell the package's installer to function in unattended mode. This option does not require any user interaction during the deployment process.

- **List Installed Hotfixes**

This option will tell the package's installer to return a list of installed hotfixes on the computer.

Note:

The Detection Agent and Inventory function provide an additional, more in-depth, listing of what is installed on to a computer.

- Other Options

This field will display the list of other extra flags that may be used for the specific deployment, but are not generic enough for all deployments to allow it to be added as a separate flag. Generally this is used for customer deployments or special case scenarios.

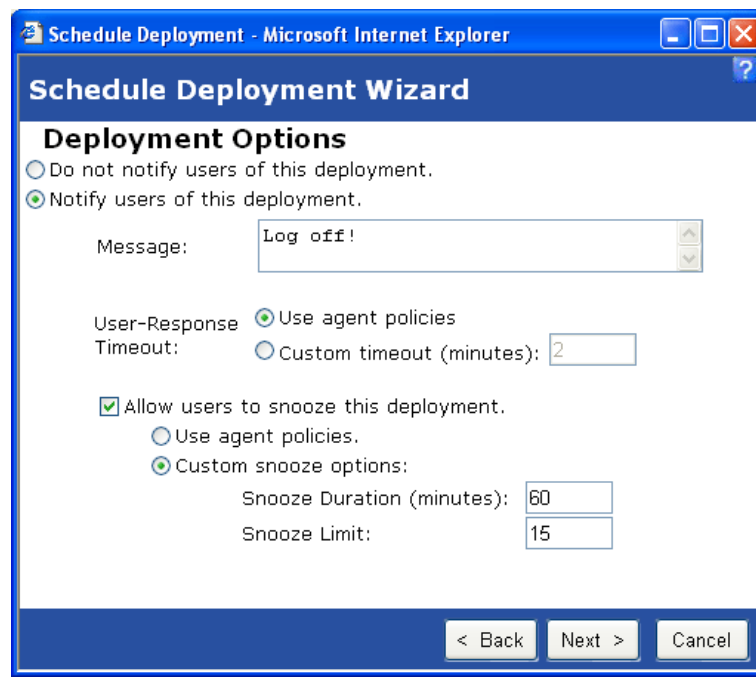
Note:

The -2 flag is often found here to indicate that the deployment's installer program may require a reboot depending if the operating system requires it.

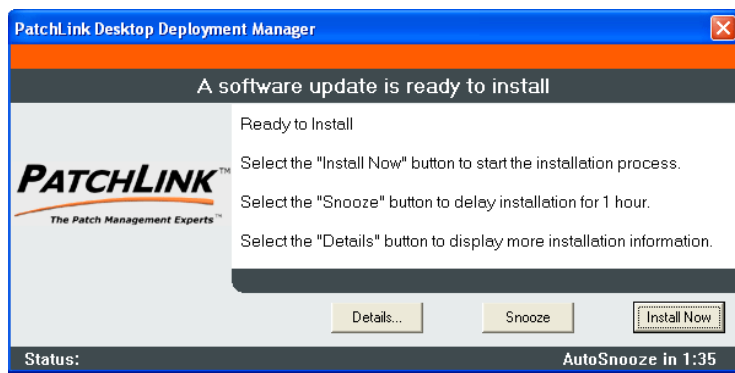
Click the **Next** button to initialize the wizard's next screen, which handles license validation if this package requires one. If the package does not require a license validation, the **Next** button initializes the wizard's next screen, which allows you to define some deployment information.

9.6 Deployment Options

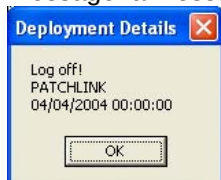
The **Deployment Options** screen initializes. Here you can select additional deployment options, notes, or details.



- Do not notify users of this deployment
If selected, the user will not be notified of the deployment, it will happen automatically.
- Notify users of this deployment
If selected, the user will be notified of the deployment



Message: a message may be inserted into the message text field to alert the user.



User Response Timeout:

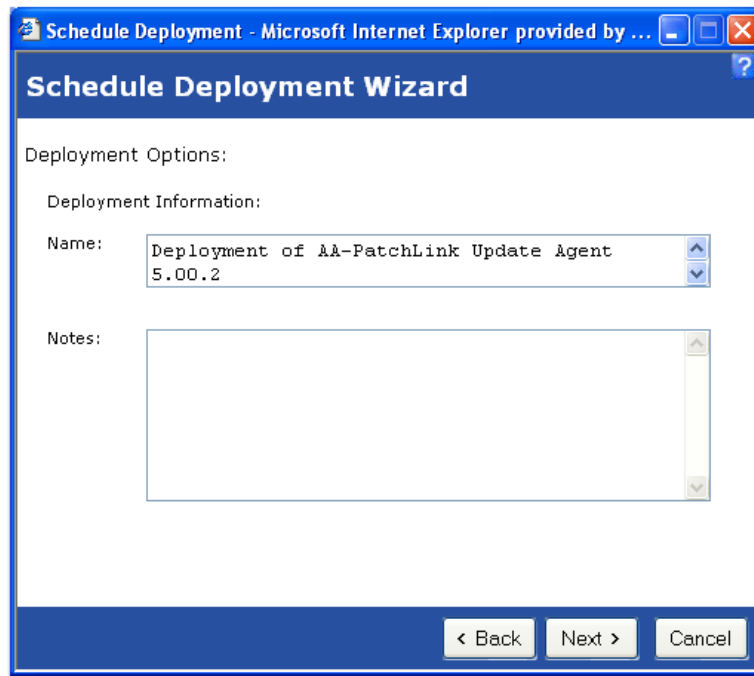
Use Agent Policies: if selected, this uses agent policies will use the pre defined agent policies.

Custom Timeout (minutes): if selected, a minute duration may be input into this field to allow a timeout user response period. If not addressed by the user in the inserted time, the package will be deployed.

After you have made your option selections, click the **Next** button to initialize the next **Deployment Options** screen.

9.7 Deployment Options

The **Deployment Options** screen initializes. Here you can select additional deployment options, notes, or details.



- **Name:** This is the name given to this deployment. The name given should be descriptive enough to summarize the deployment. This is required.
- **Notes:** This includes any additional information about the deployment that you want to note down like the expected results of this deployment, the effect that this deployment can have on any future deployments.

If there are no package flag options to choose from for the item you are deploying, clicking the **Next** button initializes the License Agreement Page **or** the Deployment Information Page, depending if there is a license agreement for what you are deploying.

Click the **Next** button to initialize an additional Deployment Options screen.

9.8 Schedule Deployment Wizard: License Information

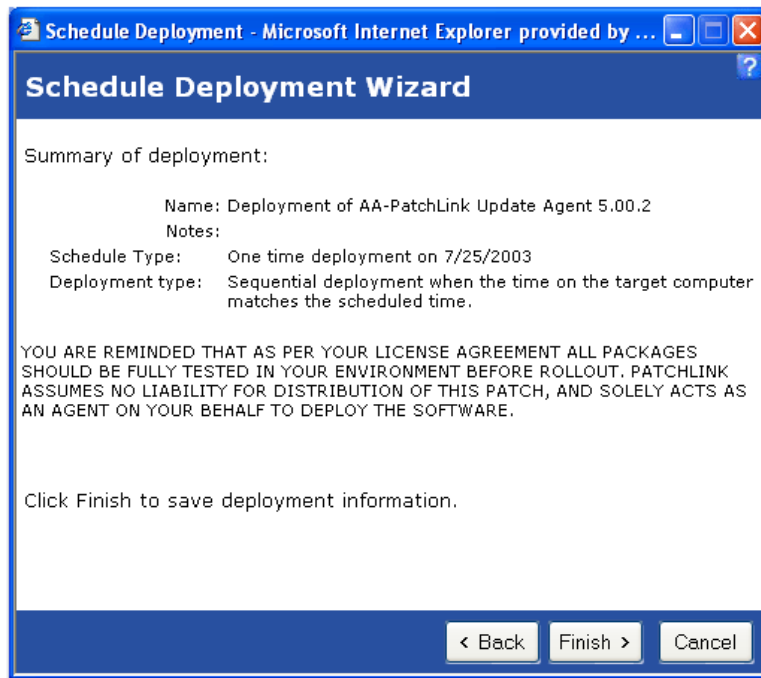
The Deployment Wizard License Information page is displayed only when a license URL is associated with the package being deployed. It will show the license URL in an imbedded frame.



Click the **I Agree** button to accept the terms and initialize the wizard's next screen, where you can define some deployment information

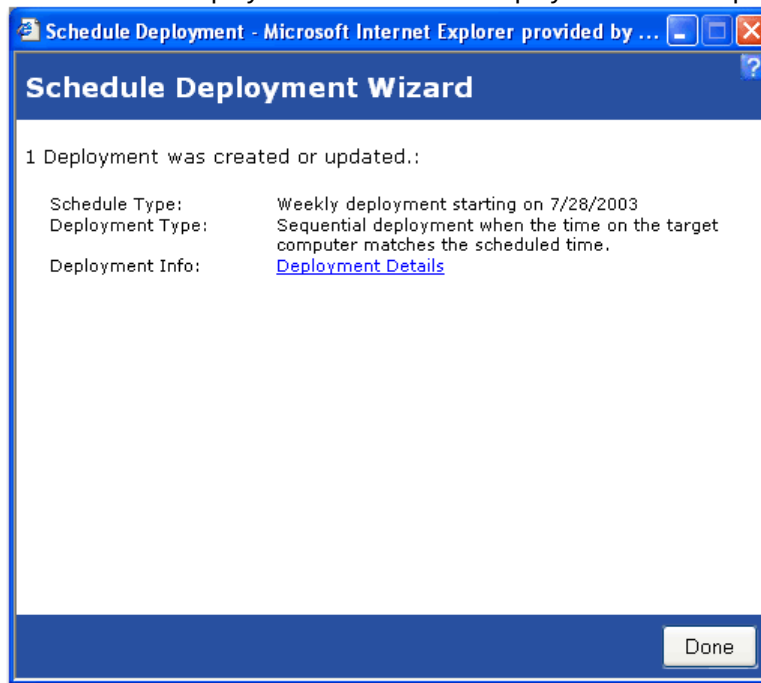
9.9 Summary

The Deployment Verification displays a simple summary of the deployment to be initialized. If any of this information is incorrect, press the **Back** button to change the values. If everything is correct, press the button **Finish** to have the wizard create the deployment.



9.10 Verification

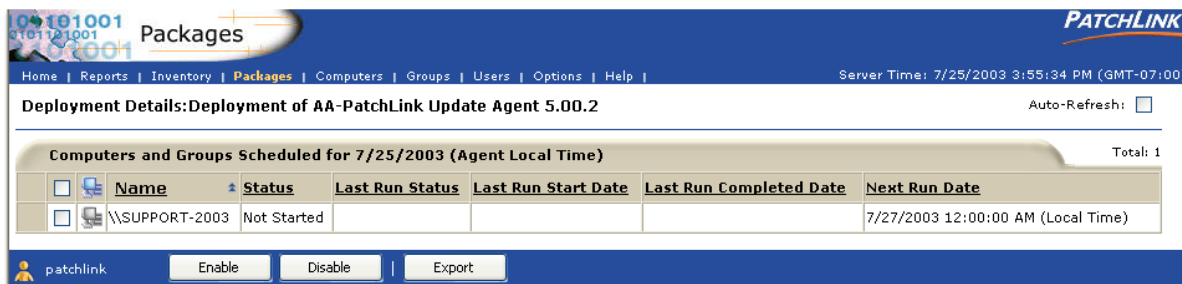
The verification screen displays the results of the deployment creation process.



- Screen Functions
 - Done
 - Closes the wizard and initializes the Deployment Details screen

- Deployment Details Link
Provides details of the deployment

Upon selection of the **Done** button, the deployment details page automatically refreshes and displays the assigned computers and groups and the status of the deployment for each. To view the group membership results for the deployment, click on the name of the group.



9.11 Package Deployments Security

The package deployments section of PLUS requires the **View Deployment Status** access right. If a user does not have the **correct** access, the access denied error message is displayed.

To be able to view the information about a distribution package requires the **View Packages** access right. If a user does not have the correct access, the hyperlink on the **Information** tab is not enabled.

To be create a deployment for the distribution package requires the **Deploy Packages** access right. If a user does not have the correct access, the **Deploy** button is disabled.

To be able to change, disable, enable, abort or remove a deployment(s) requires the **Manage Deployments** access right. If a user does not have the correct access, the **Change**, **Disable**, **Enable**, **Abort** and **Remove** buttons are disabled.

To be able to change the deployment of the **Discover Applicable Updates System Task** requires the **Manage System Tasks** access right. If a user does not have the correct access, they will receive a message indicating they do not have access.

To be able to export the distribution package's information to a comma-separated value (CSV) file requires the **Export Deployment Data** access right. If a user does not have the correct access, the **Export** button is disabled.

Contact your PatchLink Administrator for more information on **PatchLink Update Security**.

9.12 Distribution Packages Security

The Distribution Packages section of PLUS requires the [View Packages](#) access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the deployments for a distribution package requires the [View Deployments](#) access right. If a user does not have the correct access the hyperlink on the [Package Name](#) will not be displayed.

To be able to create a deployment for a selected distribution package requires the [Deploy packages](#) access right. If a user does not have the correct access the [Deploy](#) button is disabled.

To be able to create, change or remove distribution packages requires the [Manage Packages](#) access right. If a user does not have the correct access the [Add](#), [Change](#) and [Remove](#) buttons are disabled.

To export all of the distribution packages and their information to a comma-separated values (CSV) file requires the [Export Package Data](#) access right. If a user does not have the correct access the [Export](#) button is disabled.

To cache the selected (or re-cache all of the previously cached) distribution packages requires the [Cache Packages](#) access right. If a user does not have the correct access, the [Update Cache](#) button is disabled.

9.13 Package Information Security

The distribution package information section of PLUS requires the [View Packages](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the deployments of the distribution package requires the [View Deployments](#) access right. If a user does not have the correct access, the hyperlink on the [Deployments](#) tab is not enabled.

To be create a deployment for the distribution package requires the [Deploy Packages](#) access right. If a user does not have the correct access, the [Deploy](#) button is disabled.

To be able to change a local distribution package requires the [Manage Packages](#) access right. If a user does not have the correct access, the [Change](#) button is disabled.

To be able to disable or enable a distribution package requires the [Manage Packages](#) access right. If a user does not have the correct access, the [Enable](#) and [Disable](#) buttons are disabled.

To be able to export the distribution package's information to a comma-separated value (CSV) file requires the [Export Package Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

9.14 Deployments Details Security

The [Deployment Details](#) section of PLUS requires the [View Deployment Statuses](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To enable and disable a deployment assignment requires the [Manage Deployments](#) access right. If a user does not have the correct access, the [enable](#) and [disable](#) buttons are disabled.

To export the deployment details data requires the [Export Deployment Data](#) access right. If a user does not have the correct access, the [export](#) button is disabled.

Contact your PatchLink Administrator for more information on [PatchLink Update Security](#).

9.15 Deployments Results Security

The [Deployment Results](#) section of PLUS requires the [View Deployment Statuses](#) access right. If a user does not have the correct access, the access denied error message is displayed.

Contact your PatchLink Administrator for more information on [PatchLink Update Security](#).

10. Computers

Home | Vulnerabilities | Inventory | Packages | **Computers** | Groups | Users | Reports | Options | Help

The computers section of PLUS displays all computers which have an agent registered against PLUS. Clicking on a computer name will allow you to display a computer's specific information.

The screenshot shows the 'Computers' section of the PatchLink interface. It includes a search bar, a status dropdown set to 'Enabled', and a group dropdown set to 'Only Windows'. Below this is a table titled 'Enabled Computers' with columns: Computer Name, Status, Platform, OS Info, Version, and Group List. The table lists 12 computers, including WHANK, WDG-BLACK, WDG-GREEN-2, WDG-RED, WASONG, WM052K, WM10-WIN98, WOM5, WQAD105XP, WQAD10798, WQAD1K3-ENT, WQAD1K3-ADV, and WQAD1K3-SRVR. At the bottom, there are buttons for 'Previous 50', 'Display 50 rows per page', and 'Next 50'.

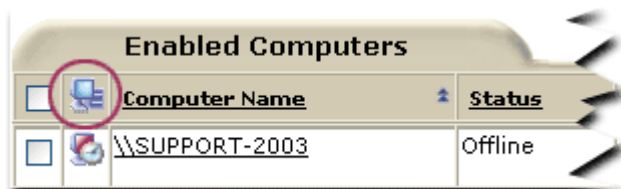
Computer Name	Status	Platform	OS Info	Version	Group List
WHANK	Idle	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.5.0.14	Win2K
WDG-BLACK	Idle	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.1.1.4	Kourosh Group, stephens , Win2K
WDG-GREEN-2	Idle	Microsoft Windows 2000 Server	Win2K-Service Pack 3	5.5.0.14	Win2K
WDG-RED	Idle	Microsoft Windows Server 2003, Standard Edition	Win2K3	5.1.1.8	Win2K3
WASONG	Offline	Microsoft Windows XP Professional	WinXP-Service Pack 1	5.1.1.12	All of Jays, WinXP
WM052K	Offline	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.1.1.6	Win2K
WM10-WIN98	Offline	Microsoft Windows 98 SE	Win98	5.1.1.6	Win98
WOM5	Idle	Microsoft Windows XP Professional	WinXP-Service Pack 1	5.1.1.12	WinXP
WQAD105XP	Offline	Microsoft Windows XP Professional	WinXP-Service Pack 1	5.1.1.5	stephens Gang, WinXP
WQAD10798	Offline	Microsoft Windows 98 SE	Win98	5.1.1.4	Kourosh Group, Win98
WQAD1K3-ENT	Offline	Microsoft Windows Server 2003, Enterprise Edition	Win2K3	5.1.1.12	All of Jays, Win2K3
WQAD1K3-ADV	Offline	Microsoft Windows 2000 Advanced Server	Win2K-Service Pack 4	5.1.1.8	All of Jays, Kourosh Group, The Brady Bunch, Win2K
WQAD1K3-SRVR	Offline	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.1.1.8	All of Jays, The Brady Bunch, Win2K

10.1 Computer Information Columns

- Computer Name**
 This displays the name of the computer. Click on the computer name to display specific information about the computer.
- Status**
 This displays the status of the computer.
- Platform**
 This displays the operating system platform the computer is running.
- OS Info**
 This displays additional information about the operating system the computer is running.

- Version
This displays the version of the agent running on the computer.
- Group List
This displays the list of groups that the computer is a member of.

10.2 Agent Status



Status	Description
	This is an idle deployment agent.
	This deployment agent is idle and has deployments
	The agent is sleeping as it is outside its hours of operation.
	The agent is sleeping as it is outside its hours of operation and has deployments in its work queue.
	This agent is currently working on a deployment (animated)
	This is an enabled detection agent that does not correspond to a registered deployment agent*.
	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes).
	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes) and has deployments in
	This agent has been disabled.

Additional information may be displayed by hovering your mouse pointer over an enabled icon.

To display additional information about the computer, click on the name of the actual computer. This performs the same function as selecting the computer and clicking on the View button on the Action Menu.

* This usually means that either the deployment agent was removed from PLUS or there has been a problem in registering the deployment agent. For more information on this check the agent installation section.

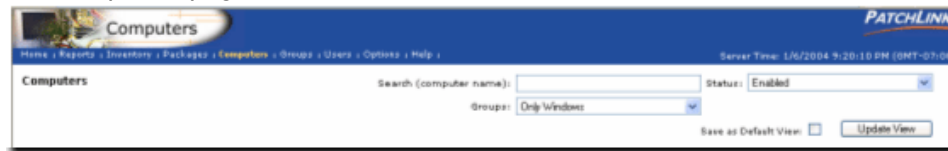
10.3 Page Functions

- Display and Hide

Click the  to display additional information and statistics about the represented item. Click the  to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (, ) is only available for Microsoft Internet Explorer at this time.

- Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Computers page header.



- Search

Search (computer name):

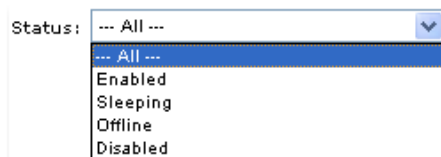
You may search computers for more granular results by entering the computer name text into the **Search** field and clicking on the  Update View button.

This will return the computer having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

- Status

Filter by status using the dropdown menu and click on the  Update View button.



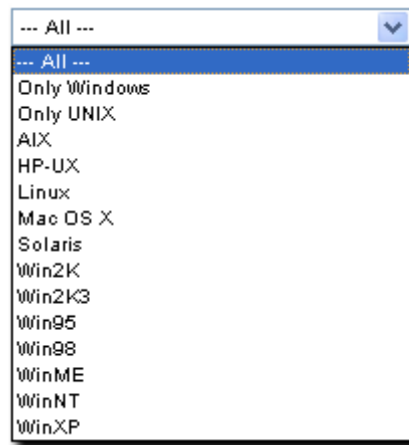
This allows the user to search on enabled, sleeping, offline, and disabled systems that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

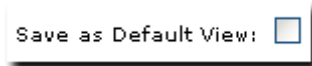
- Groups

Filter by group using the dropdown menu and click on the  Update View button.

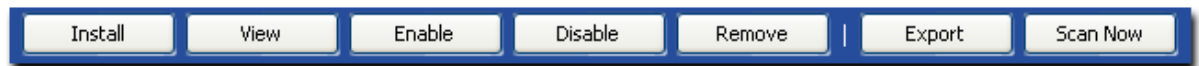


This allows the user to search on any user defined or server defined groups that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

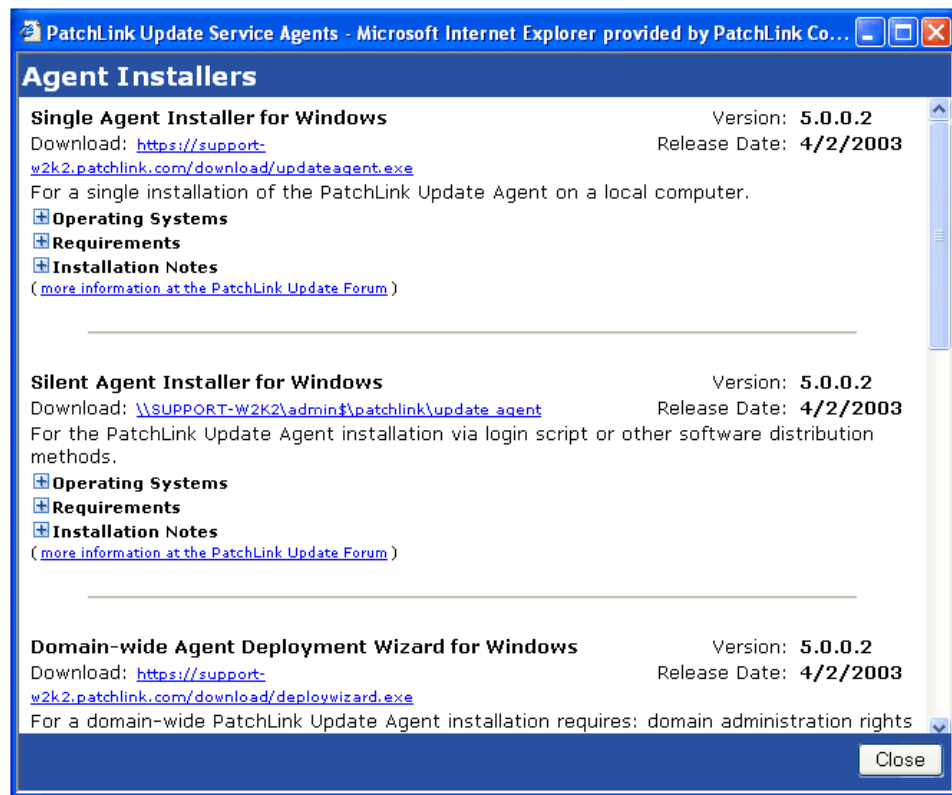


10.4 Action Menu



- Install

Click on the Install button to display the list of agent installers that can be used to register computers to PLUS. See Section 3.6, Agent Management Center for more details on Agents and installing them.



Single Agent Installer for Windows – Local Machine

Agent Installation can be launched from any computer within your network. First log into the PatchLink Update Server administration interface, then click Computers, and press the Add button.

At this point, select the Single Agent Installer for Windows hyperlink to start downloading. Depending upon your bandwidth constraints this will take between a couple of seconds and a few minutes. You may also be presented with a screen indicating that the executable you are downloading was created and digitally signed by PatchLink Corporation.

Once downloaded, run UPDATEAGENT.EXE to actually start the process of agent installation.

The steps are as follows:

Initialization Step

Please wait while the deployment wizard is initialized on this computer.

Welcome Screen

Press the Next> button to begin the agent deployment process

License Agreement

Please read the license agreement carefully, this is the same agreement provided during server installation, but must be acknowledged by all administrators of the system. Once you have read the agreement, select the “I accept the terms” or “I do not accept the terms” option.

Press the Next> button to continue the deployment process or the Cancel button to abort.

Agent Registration

In the Host URL field, enter the URL that you use to access your PatchLink Update Server from your web browser, including its protocol prefix (http:// or https:// for a secure server). The serial number entry field must be filled out completely with the SAME serial number that you used when your PatchLink Update Server was installed. It is extremely important that you use the same serial number – if you provide any other valid serial number or evaluation serial number, your newly installed agents will be unable to communicate at all.

If your Local Area Network configuration requires the use of a proxy server to access the PatchLink Update Server, you can enter the proxy connection string in the third entry field, otherwise just leave it blank. Please be sure to enter a valid proxy server name and port – e.g.: http://myproxy.mycompany.com:8080.

PLEASE NOTE: for environments where a proxy server is required to access the Internet, you may be wondering whether to enter proxy information or not. However please be sure to ONLY enter proxy information if your agents will be required to talk *via the proxy server* in order to communicate with your PatchLink Update Server. In most LAN environments, “Proxy Bypass” is used to access web servers within the corporate network – so that the proxy server only has to deal with outbound access to the World Wide Web.

Install Summary

If you selected Local Machine install, this is the last step of the install procedure before copying files.

Press Begin to start the installation process onto this computer.

Setup Complete

The final wizard screen will confirm that the Update Agent was successfully installed onto this computer. Any errors that occurred will be shown in red text, please recheck your serial number and Host URL and try again.

Silent installer

The Silent Installer is designed for use with log in scripts. The program is stored on a public directory. A sample log in script can be found on the PLUS server, which demonstrates how it is most effectively used.

Windows 95, Windows 98 and Windows ME computers do not share resources automatically on the network, and therefore it is not possible to automatically install the agent remotely from another computer to any generic workstation. In practice the best deployment method for these types of workstations – and indeed for your Windows2000 Professional workstations – is to use a Network Login Script command to launch the agent installer.

Should you opt to use Network Login Script as your exclusive mechanism of deploying the agent to all workstations and servers, you will gain the added benefit of having any new machine that logs into the network automatically inventoried and patched by the system. This means that fresh machines straight from the manufacturer can now be added to your network and then brought up to the latest patch level in a matter of minutes using the PatchLink Update technology.

To setup the Update Agent software to be installed automatically as computers log in to your network, you will need to first copy the installation files onto the network and then use a simple batch file to run the install with the appropriate options from the network login script.

The \\WINNT\\PatchLink\\Update Agent\\ directory and its subdirectories contain a complete installable image of the Update Agent, including the associated Windows Installer (MSI) dependencies. This directory can be copied out to any NT, NetWare or UNIX server that your workstations can access and that is normally available during the network login process.

For example, use the command:

XCOPY "c:\\winnt\\patchlink\\update agent" [\\serv\\share\\update](#) /s

To copy the whole install configuration from your Update Server box over to a network share [\\serv\\share](#).

Once the code is out on the network, your next step is to call a simple batch file that runs the setup program with the appropriate arguments. This can be done merely by calling the file NetInstall.BAT which is included with the agent installation files – or you may wish to customize that Batch File to meet your particular network / workstation configuration.

In the previous example, your Network Login Script would just need the following additional lines added to it:

**CD [\\serv\\share\\update](#)
[\\serv\\share\\update\\netinstall.bat](#)**

Please refer to the documentation for your own network operating system for specific instructions on calling batch file programs and shell commands for the exact syntax that should be used.

It is also possible just to run the installation program directly using

setup.exe -s

...this will run the setup program in silent mode using the SETUP.ISS silent response file. Be sure to copy SETUP.BAK to SETUP.ISS before using this technique for the first time, and edit the URL and Serial Number if necessary to make the silent install work from all locations (e.g. substitute a DNS name instead of the IP address of the Update Server).

MSI installer

The MSI installer is designed for windows networks that use the windows software installer mechanism. The MSI installer can be edited to include the PLUS server name and serial number. In this way, the agent can be deployed through the use of Group Policy Objects.

Domain Wide Installation

The Domain scan requires Domain Administration privileges in the Enterprise, per Domain, in order to enumerate all the Domains and the computers within those Domains throughout the Enterprise. By placing these credentials in the Domain scan Username and Password fields, an Administrator can enumerate all the computers within every Domain in the Enterprise.

The Domain Scan will Find and list all the Domains within an Enterprise. Once the Domains have been discovered, a Search a Domain job can be initiated to enumerate all the computers within those Domains. When the computers have been enumerated for their respective Domains, selecting those computers or Domains, an agent can be installed to those computers.

Domain-Wide Deployment must be launched from a Windows2000 or Windows XP machine which has been logged on to the network with a domain administrator equivalent account. This will allow agents to be remote deployed to other computers within the network.

First log into the PatchLink Update Server administration interface, then click Computers, and press the Install button. On the Agent installers' screen, select the [Domain-Wide Agent Deployment Wizard for Windows](#) hyperlink and the Deployment Wizard will start downloading. Depending upon your bandwidth constraints this will take between a couple of seconds and a few minutes. You may also be presented with a screen indicating that the executable you are downloading was created and digitally signed by PatchLink Corporation.

Once downloaded, run DEPLOYWIZARD.EXE to install the application which will allow you to run remote agent deployment.

Installation Step

A simple InstallShield wizard is used to install the Agent Deployment Wizard for Windows onto your computer. Merely accept the license agreement and allow the setup program to complete. Note that this only has to be done one time – and then the wizard can be run over and over again.

To run the Agent Deployment Wizard again, merely click on the desktop shortcut that is created by the setup program.

The wizard steps are as follows:

Welcome Screen

Press the Next> button to begin the agent deployment process

License Agreement

Please read the license agreement carefully, this is the same agreement provided during server installation, but must be acknowledged by all administrators of the system. Once you have read the agreement, select the "I accept the terms" or "I do not accept the terms" option.

Press the Next> button to continue the deployment process or the Cancel button to abort.

Agent Registration

In the Host URL field, enter the URL that you use to access your PatchLink Update Server from your web browser, including its protocol prefix (http:// or https:// for a secure server). The serial number entry field must be filled out completely with the SAME serial number that you used when your PatchLink Update Server was installed. It is extremely important that you use the same serial number – if you provide any other valid serial number or evaluation serial number, your newly installed agents will be unable to communicate at all.

If your Local Area Network configuration requires the use of a proxy server to access the PatchLink Update Server, you should see the "Use proxy server" option checked. Should you have any unusual proxy server requirements, please check this box and make sure your proxy server address and port are correct before continuing.

Next choose the "Domain Wide Installation" option to install onto multiple computers within your domain. Should this option be grayed out, make sure that you are logged in with an administrator equivalent account and also that ADMIN\$ shares are available on your domain controller and the local computer you are rolling out from. In order to have the agent successfully deployed using this technique, the target computer must be a current member of

the domain, be currently powered on and also have its ADMIN\$ shares available. Specifically this excludes all Windows ME, Windows 98 and Windows 95 computers that do not provide administrative shares on the network.

PLEASE NOTE: for environments where a proxy server is required to access the Internet, you may see the “Use Proxy Server” option checked. However please be sure to only leave the option checked if your agents will be required to talk via the proxy server in order to communicate with your PatchLink Update Server. In most LAN environments, “Proxy Bypass” is used to access web servers within the corporate network – so that the proxy server only has to deal with outbound access to the World Wide Web.

Click Next> to specify the user account under which the agent will be installed.

Domain Administrator Information

Enter the username and password of the currently logged in administrative user within your domain. The installation program will be installing the agent using this name and password on the remote computers, and there should be no domain policies in place forbidding this user from logging on as a service (SeLogonAsService right).

Specify Computers

In this version you can either select the computers to receive the agent from a graphical list that shows the machine type, installed status and so forth – or alternatively just specify the names of machines separated by commas. We recommend that you use the graphical list of computers to select machines under virtually all circumstance. Should you wish to roll out only one known computer within a very large domain, and you know the exact computer name, you may find the alternate method useful.

Once you have selected the computers to be installed with the Update Agent, press Next> in order to initiate the deployment process. At this time the Deployment Wizard will map drives to each computer in turn, copy over the installation files and then attempt to start the setup process using a system task. For WindowsNT computers, you may need to shutdown and restart the computer for the Agent Install process to complete on that machine.

Install Summary

If you selected Local Machine install, this is the last step of the install procedure before copying files.

Press Begin to start the installation process onto this computer.

Deployment Complete

The final wizard screen will confirm that the Update Agent was successfully installed onto this computer. Any errors that occurred will be shown in red text, please recheck your serial number and Host URL and try again. As the deployment process continues, a ROLLOUT.LOG file is generated within the \Program Files\PatchLink\Update Agent sub-directory. At the end of installation you will be notified if all computers were deployed to successfully.

If any problems occurred, check the ROLLOUT.LOG in order to identify which computers were unable to be reached by the deployment wizard. This may be because the computer was powered off, the domain information is corrupt or outdated, or because ADMIN\$ shares have temporarily been disabled on that computer. It is also possible that you may be out of disk space on the target computer or other install-related errors could have occurred: in this case you will be referred to the INSTALL.LOG file on the target system.

For any computer within the domain that is unable to receive the agent via rollout, you can always opt to install that node via a local machine installation.

In larger multi-domain environments, the use of Network Login Scripts is strongly encouraged. Refer to the product documentation for more details.

PatchLink Distribution Point

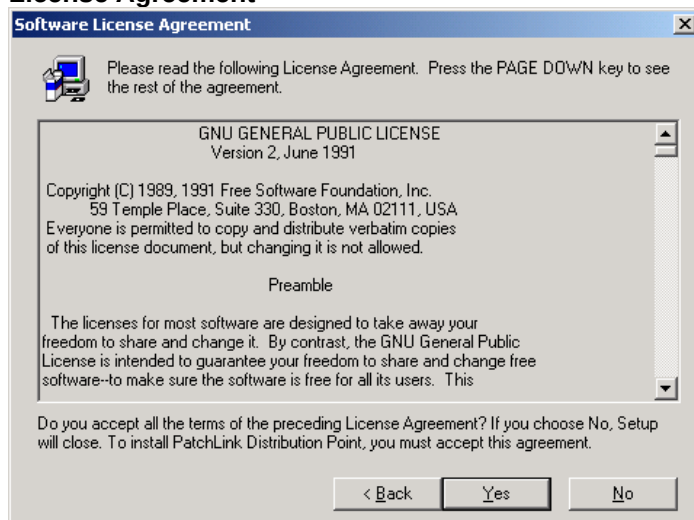
Provides a quick and easy way to add remote package cache capabilities to any server computer within your wide area network. Based on the SQUID NT v2.5 open source based product, this software provides you with a turnkey content caching solution where none previously existed. It is recommended that PatchLink Distribution Point should be installed on server computers within your environment that are permanently connected to your network. Installing on a workstation is also possible, however since that workstation becomes a gateway for communication between agent computers and the Update Server, it is a good idea to make sure that computer is permanently attached to the WAN and always live on the network. The default proxy port for PatchLink Distribution Point is 25253.

Once a Distribution Point has been installed in a remote office, new agents at that location can be configured to communicate through the Distribution Point by specifying :25253 as the proxy value during agent installation. Proxy settings for existing agents can also be modified by launching the PatchLink Update control panel applet and pushing the "Proxy" button.

- **Running the Installation**
The PatchLink Distribution Point install executable is called PLDISTPT.EXE and can be downloaded by logging in to the web based administration interface and clicking on the Computers section of the product, then pushing the Install button on the bottom left of that screen and selecting the download link for "PatchLink Distribution Point 2.0"..

Once the setup program is downloaded, double click or run the PLDISTPT.EXE file on the computer on which the Distribution Point is to be installed.

License Agreement

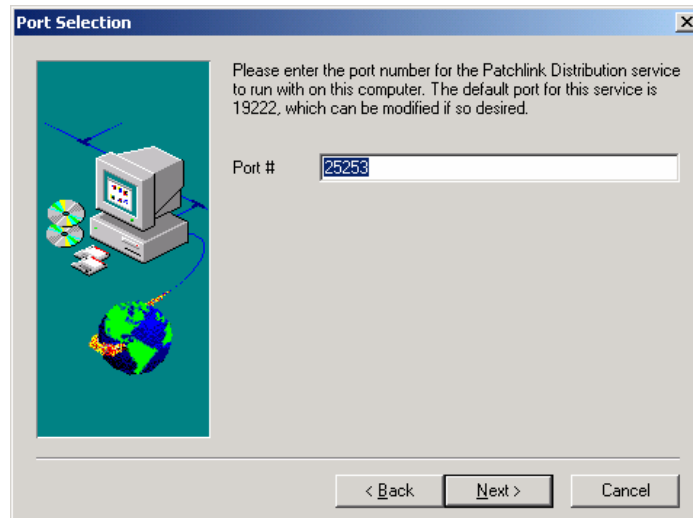


The first screen of the installation program displays the GNU GENERAL PUBLIC LICENSE agreement under which you are entitled to use this piece of software, which has been derived from the SQUID for NT Version 2.5 product.

Please note that this open source license agreement applies only to the PatchLink Distribution Point product. All other parts of the PatchLink solution are covered by your existing EULA and/or MLA license documents.

Press YES to acknowledge the license agreement.

Selection of Port

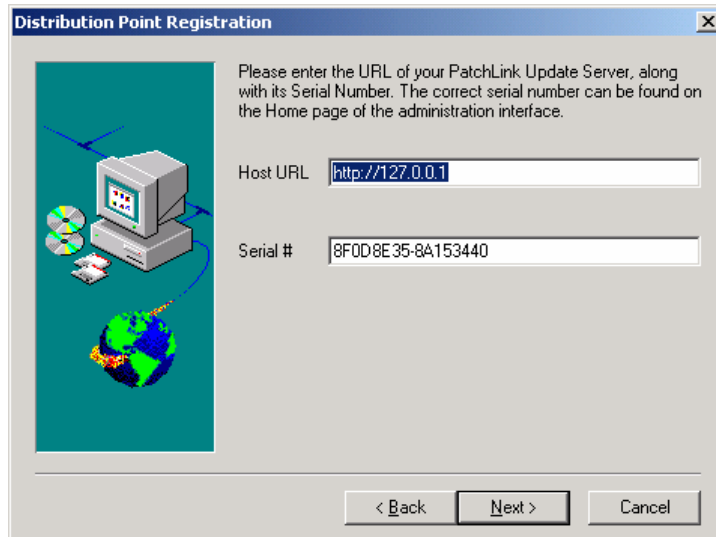


The PatchLink Distribution Point installation requires that you select a TCP/IP port that this service can run on. Typical proxy service ports are 8080, 8081 and so forth. By default this port value is set to 25253 – however you can specify any numeric value that you wish that doesn't conflict with other known services that you are using on this box.

Enter the desired port number, or accept the default value.

Press Next to continue.

Registration Parameters



The Distribution Point installer will attempt to register this proxy with its corresponding PatchLink Update server.

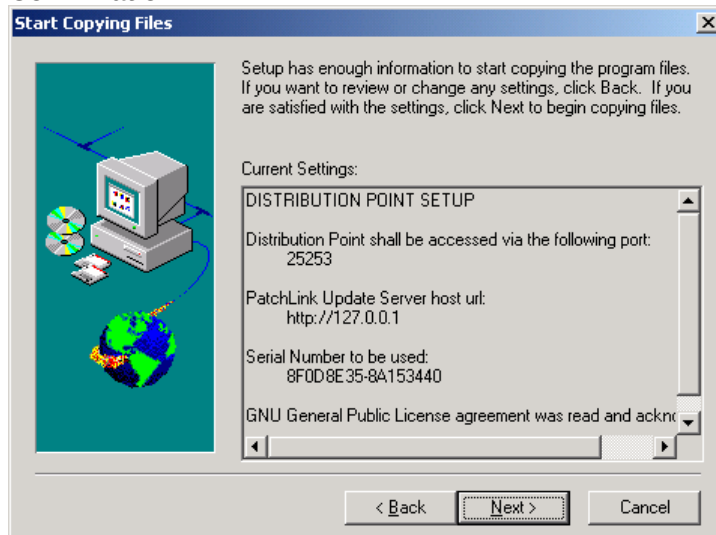
We recommend that you enter your Update Server URL and Serial Number at this time so that registration can be completed – if you choose not to enter this information correctly or do not know the information; your new Distribution Point will not be included on the list of distribution points supplied to Agent computers during network path optimization tasks.

Enter the PatchLink Update host url (optional)

Enter the Serial Number (optional)

Press Next to continue.

Confirmation



This screen merely confirms your chosen installation parameters. If you wish to change any of the listed values, press Back and make your modifications at this time.

Press Next to complete installation.

Post Installation Configuration

Once installation is completed, the program files and configuration files can be found in the **C:\program files\patchlink\Distribution Point** sub-directory on the target computer. The service that has been installed and automatically started on the computer is called **PatchLink_Distribution**.

The PatchLink_Distribution service can be started and stopped like any other Windows service by going to Control Panel -> Administrative Tools -> Services. Note that when the service is running, agents may obtain their patch files from the Distribution Point – however when the service is stopped or the computer is offline for any reason (power management, suspend mode, etc) all agent communications will be suspended through that Distribution Point. For this reason we recommend that a dedicated computer that is permanently connected to the network backbone should be used for a Distribution Point.

Advanced configuration options can now be modified, if so desired, by editing the two configuration files located in the **C:\program files\patchlink\Distribution Point\etc** subdirectory:

SQUID.CONF - which contains all cache configuration parameters
MIME.CONF - controls what content types are handled

These options are explained in detail in the next two sections.

Cache Configuration Options – SQUID.CONF

NOTE: The following list is a relevant subset of all available options. Refer to SQUID.CONF.DEFAULT for a complete listing of all available options for the product.

It is not recommended that you alter the default configuration options set by the installation program, and doing so may require you to have to re-install if you require support from the PatchLink Support team.

Network Options

http_port

The socket addresses where SQUID will listen for HTTP client requests. You may specify multiple socket addresses. There are three forms: port alone, hostname with port, and IP address with port. If you specify a hostname or IP address, then SQUID binds the socket to that specific address. This replaces the old 'tcp_incoming_address' option. Most likely, you do not need to bind to a specific address, so you can use the port number alone.

The default port number is 3128.

If you are running SQUID in accelerator mode, then you probably want to listen on port 80 also.

The -a command line option will override the *first* port number listed here. That option will NOT override an IP address, however.

You may specify multiple socket addresses on multiple lines.

If you run SQUID on a dual-homed machine with an internal and an external interface then we recommend you to specify the internal address:port in `http_port`. This way SQUID will only be visible on the internal address.

icp_port:

The port number where SQUID sends and receives ICP queries to and from neighbor caches. Default is 3130. To disable use "0". May be overridden with `-u` on the command line.

htcp_port

The port number where SQUID sends and receives HTCP queries to and from neighbor caches. Default is 4827. To disable use "0".

mcast_groups

This tag specifies a list of multicast groups which your server should join to receive multicasted ICP queries.

NOTE! Be very careful what you put here! Be sure you understand the difference between an `ICP_query_` and an `ICP_reply_`. This option is to be set only if you want to RECEIVE multicast queries. Do NOT set this option to SEND multicast ICP (use `cache_peer` for that). ICP replies are always sent via unicast, so this option does not affect whether or not you will receive replies from multicast group members.

You must be very careful to NOT use a multicast address which is already in use by another group of caches.

If you are unsure about multicast, please read the Multicast chapter in the SQUID FAQ (<http://www.SQUID-cache.org/FAQ/>).

Usage: `mcast_groups 239.128.16.128 224.0.1.20`
By default, SQUID doesn't listen on any multicast groups.

udp_incoming_address**udp_outgoing_address**

`udp_incoming_address` is used for the ICP socket receiving packets from other caches.

`udp_outgoing_address` is used for ICP packets sent out to other caches. The default behavior is to not bind to any specific address.

A `udp_incoming_address` value of 0.0.0.0 indicates that SQUID should listen for UDP messages on all available interfaces.

If `udp_outgoing_address` is set to 255.255.255.255 (the default) then it will use the same socket as `udp_incoming_address`. Only change this if you want to have ICP queries sent using another address than where this SQUID listens for ICP queries from other caches.

NOTE, `udp_incoming_address` and `udp_outgoing_address` can not have the same value since they both use port 313

Options Which Affect the Neighbor Selection Algorithm

cache_peer

To specify other caches in a hierarchy, use the format: cache_peer hostname type http_port icp_port. For example, proxy icp

hostname	type	port	port	options
-----	-----	-----	-----	-----
cache_peer parent.foo.net	parent	3128	3130	[proxy-only]
cache_peer sib1.foo.net	sibling	3128	3130	[proxy-only]
cache_peer sib2.foo.net	sibling	3128	3130	[proxy-only]

type: either 'parent', 'sibling', or 'multicast'.

proxy_port: The port number where the cache listens for proxy requests.

icp_port: Used for querying neighbor caches about objects. To have a non-ICP neighbor specify '7' for the ICP port and make sure the neighbor machine has the UDP echo port enabled in its /etc/inetd.conf file.

options: proxy-only

weight=n; ttl=n; no-query; default; round-robin; multicast-responder; closest-only; no-digest; no-netdb-exchange; no-delay; login=user:password | PASS | *:password; connect-timeout=nn; digest-url=url; allow-miss; max-conn

use 'proxy-only' to specify that objects fetched from this cache should not be saved locally. use weight=n' to specify a weighted parent. The weight must be an integer. The default weight is 1, larger weights are favored more.

use 'ttl=n' to specify a IP multicast TTL to use when sending an ICP queries to this address. Only useful when sending to a multicast group. Because we don't accept ICP replies from random hosts, you must configure other group members as peers with the 'multicast-responder' option below.

use 'no-query' to NOT send ICP queries to this neighbor. use 'default' if this is a parent cache which can be used as a "last-resort." You should probably only use 'default' in situations where you cannot use ICP with your parent cache(s). use 'round-robin' to define a set of parents which should be used in a round-robin fashion in the absence of any ICP queries.

'multicast-responder' indicates that the named peer is a member of a multicast group. ICP queries will not be sent directly to the peer, but ICP replies will be accepted from it.

'closest-only' indicates that, for ICP_OP_MISS replies, we'll only forward LOSEST_PARENT_MISSES and never FIRST_PARENT_MISSES. use 'no-digest' to NOT request cache digests from this neighbor.

'no-netdb-exchange' disables requesting ICMP RTT database (NetDB) from the neighbor.

use 'no-delay' to prevent access to this neighbor from influencing the delay pools.

use 'login=user:password' if this is a personal/workgroup proxy and your parent requires proxy authentication.

Note: The string can include URL escapes (i.e. %20 for spaces). This also means that % must be written as %%. use 'login=PASS' if users must authenticate against the upstream proxy. This will pass the users credentials as they are to the peer proxy. This only works for the Basic HTTP authentication scheme. Note: To combine this with proxy_auth both proxies must share the same user database as HTTP only allows for one proxy login. Also be warned that this will expose your users proxy password to the peer. USE WITH CAUTION use 'login=*.password' to pass the username to the upstream cache, but with a fixed password. This is meant to be used when the peer is in another administrative domain, but it is still needed to identify each user.

The star can optionally be followed by some extra information which is added to the username. This can be used to identify this proxy to the peer, similar to the login=username:password option above.

use 'connect-timeout=nn' to specify a peer specific connect timeout (also see the peer_connect_timeout directive)

use 'digest-url=url' to tell SQUID to fetch the cache digest (if digests are enabled) for this host from the specified URL rather than the SQUID default location. use 'allow-miss' to disable SQUID's use of only-if-cached when forwarding requests to siblings. This is primarily useful when icp_hit_stale is used by the sibling. To extensive use of this option may result in forwarding loops, and you should avoid having two-way peerings with this option. (for example to deny peer usage on requests from peer by denying cache_peer_access if the source is a peer)

use 'max-conn' to limit the amount of connections SQUID may open to this peer.

NOTE: non-ICP neighbors must be specified as 'parent'.

cache_peer_domain

Use to limit the domains for which a neighbor cache will be queried. Usage:

```
cache_peer_domain cache-host domain [domain ...]
cache_peer_domain cache-host !domain
```

For example, specifying cache_peer_domain parent.foo.net.edu

has the effect such that UDP query packets are sent to 'bigserver' only when the requested object exists on a server in the .edu domain. Prefixing the domainname with '!' means that the cache will be queried for objects NOT in that domain.

NOTE: * Any number of domains may be given for a cache-host, either on the same or separate lines.

* When multiple domains are given for a particular cache-host, the first matched domain is applied.

* Cache hosts with no domain restrictions are queried for all requests.

* There are no defaults.

* There is also a 'cache_peer_access' tag in the ACL section.

neighbor_type_domain

usage: neighbor_type_domain neighbor parent|sibling domain domain ...

Modifying the neighbor type for specific domains is now possible. You can treat some domains differently than the default neighbor type specified on the 'cache_peer' line.

Normally it should only be necessary to list domains which should be treated differently because the default neighbor type applies for hostnames which do not match domains listed here.

EXAMPLE:

```
cache_peer parent cache.foo.org 3128 3130
neighbor_type_domain cache.foo.org sibling .com .net
neighbor_type_domain cache.foo.org sibling .au .de
```

icp_query_timeout (msec)

Normally SQUID will automatically determine an optimal ICP query timeout value based on the round-trip-time of recent ICP queries. If you want to override the value determined by SQUID, set this 'icp_query_timeout' to a non-zero value. This value is specified in MILLISECONDS, so, to use a 2-second timeout (the old default), you would write:

```
icp_query_timeout 2000
```

maximum_icp_query_timeout (msec)

Normally the ICP query timeout is determined dynamically. But sometimes it can lead to very large values (say 5 seconds). Use this option to put an upper limit on the dynamic timeout value. Do NOT use this option to always use a fixed (instead of a dynamic) timeout value. To set a fixed timeout see the 'icp_query_timeout' directive.

mcast_icp_query_timeout (msec)

For Multicast peers, SQUID regularly sends out ICP "probes" to count how many other peers are listening on the given multicast address. This value specifies how long SQUID should wait to count all the replies. The default is 2000 msec, or 2 seconds.

dead_peer_timeout (seconds)

This controls how long SQUID waits to declare a peer cache as "dead." If there are no ICP replies received in this amount of time, SQUID will declare the peer dead and not expect to receive any further ICP replies. However, it continues to send ICP queries, and will mark the peer as alive upon receipt of the first subsequent ICP reply.

This timeout also affects when SQUID expects to receive ICP replies from peers. If more than 'dead_peer' seconds have passed since the last ICP reply was received, SQUID will not expect to receive an ICP reply on the next query. Thus, if your time between requests is greater than this timeout, you will see a lot of requests sent DIRECT to origin servers instead of to your parents.

hierarchy_stoplist

A list of words which, if found in a URL, cause the object to be handled directly by this cache. In other words, use this to not query neighbor caches for certain objects. You may list this option multiple times.

no_cache

A list of ACL elements which, if matched, cause the request to not be satisfied from the cache and the reply to not be cached. In other words, use this to force certain objects to never be cached. You must use the word 'DENY' to indicate the ACL names which should NOT be cached.

We recommend you to use the following two lines.

```
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
```

Options which affect the Cache Size

cache_mem (bytes)

NOTE: THIS PARAMETER DOES NOT SPECIFY THE MAXIMUM PROCESS SIZE. IT ONLY PLACES A LIMIT ON HOW MUCH ADDITIONAL MEMORY SQUID WILL USE AS A MEMORY CACHE OF OBJECTS. SQUID USES MEMORY FOR OTHER THINGS AS WELL.

'cache_mem' specifies the ideal amount of memory to be used for:

- * In-Transit objects
- * Hot Objects
- * Negative-Cached objects

Data for these objects are stored in 4 KB blocks. This parameter specifies the ideal upper limit on the total size of 4 KB blocks allocated. In-Transit objects take the highest priority.

In-transit objects have priority over the others. When additional space is needed for incoming data, negative-cached and hot objects will be released. In other words, the negative-cached and hot objects will fill up any unused space not needed for in-transit objects.

If circumstances require, this limit will be exceeded. Specifically, if your incoming request rate requires more than 'cache_mem' of memory to hold in-transit objects, SQUID will exceed this limit to satisfy the new requests. When the load decreases, blocks will be freed until the high-water mark is reached. Thereafter, blocks will be used to store hot objects.

cache_swap_low (percent, 0-100)

cache_swap_high (percent, 0-100)

The low- and high-water marks for cache object replacement. Replacement begins when the swap (disk) usage is above the low-water mark and attempts to maintain utilization near the low-water mark. As swap utilization gets close to high-water mark object eviction becomes more aggressive. If utilization is close to the low-water mark less replacement is done each time.

Defaults are 90% and 95%. If you have a large cache, 5% could be hundreds of MB. If this is the case you may wish to set these numbers closer together.

maximum_object_size (bytes)

Objects larger than this size will NOT be saved on disk. The value is specified in kilobytes, and the default is 4MB. If you wish to get a high BYTES hit ratio, you should probably increase this (one 32 MB object hit counts for 3200 10KB hits). If you wish to increase speed more than your want to save bandwidth you should leave this low.

NOTE: if using the LFUDA replacement policy you should increase this value to maximize the byte hit rate improvement of LFUDA! See replacement_policy below for a discussion of this policy.

minimum_object_size (bytes)

Objects smaller than this size will NOT be saved on disk. The value is specified in kilobytes, and the default is 0 KB, which means there is no minimum.

maximum_object_size_in_memory (bytes)

Objects greater than this size will not be attempted to kept in the memory cache. This should be set high enough to keep objects accessed frequently in memory to improve performance whilst low enough to keep larger objects from hoarding cache_mem .

ipcache_size (number of entries)

ipcache_low (percent)

ipcache_high (percent)

The size, low-, and high-water marks for the IP cache.

fqdn_cache_size (number of entries)
Maximum number of FQDN cache entries.

cache_replacement_policy

The cache replacement policy parameter determines which objects are evicted (replaced) when disk space is needed.

lru : SQUID's original list based LRU policy
heap GDSF : Greedy-Dual Size Frequency
heap LFUDA: Least Frequently Used with Dynamic Aging
heap LRU : LRU policy implemented using a heap

Applies to any cache_dir lines listed below this.

The LRU policies keeps recently referenced objects.

The heap GDSF policy optimizes object hit rate by keeping smaller popular objects in cache so it has a better chance of getting a hit. It achieves a lower byte hit rate than LFUDA though since it evicts larger (possibly popular) objects.

The heap LFUDA policy keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached.

Both policies utilize a dynamic aging mechanism that prevents cache pollution that can otherwise occur with frequency-based replacement policies.

NOTE: if using the LFUDA replacement policy you should increase the value of maximum_object_size above its default of 4096 KB to maximize the potential byte hit rate improvement of LFUDA.

For more information about the GDSF and LFUDA cache replacement policies see <http://www.hpl.hp.com/techreports/1999/HPL-1999-69.html> and <http://fog.hpl.external.hp.com/techreports/98/HPL-98-173.html>.

memory_replacement_policy

The memory replacement policy parameter determines which objects are purged from memory when memory space is needed.

See cache_replacement_policy for details.

Logfile PathNames and Cache Directory

cache_dir

You can specify multiple cache_dir lines to spread the cache among different disk partitions.

Type specifies the kind of storage system to use. Only "ufs" is built by default. To enable any of the other storage systems see the --enable-storeio configure option.

'Directory' is a top-level directory where cache swap files will be stored. If you want to use an entire disk for caching, then this can be the mount-point directory. The directory must exist and be writable by the SQUID process. SQUID will NOT create this directory for you.

The ufs store type:

"ufs" is the old well-known SQUID storage format that has always been there.

cache_dir ufs Directory-Name Mbytes L1 L2 [options] 'Mbytes' is the amount of disk space (MB) to use under this directory. The default is 100 MB. Change this to suit your configuration. Do NOT put the size of your disk drive here. Instead, if you want SQUID to use the entire disk drive, subtract 20% and use that value.

'Level-1' is the number of first-level subdirectories which will be created under the 'Directory'. The default is 16.

'Level-2' is the number of second-level subdirectories which will be created under each first-level directory. The default is 256.

The aufs store type:

"aufs" uses the same storage format as "ufs", utilizing POSIX-threads to avoid blocking the main SQUID process on disk-I/O. This was formerly known in SQUID as async-io. cache_dir aufs Directory-Name Mbytes L1 L2 [options] see argument descriptions under ufs above

The awin32 store type:

"awin32" uses the same storage format as "ufs", utilizing WIN32-threads to avoid blocking the main SQUID process on disk-I/O. This was formerly known in SQUID as async-io. cache_dir awin32 Directory-Name Mbytes L1 L2 [options] see argument descriptions under ufs above

The diskd store type:

"diskd" uses the same storage format as "ufs", utilizing a separate process to avoid blocking the main SQUID process on disk-I/O.

cache_dir diskd Directory-Name Mbytes L1 L2 [options] [Q1=n] [Q2=n] see argument descriptions under ufs above Q1 specifies the number of unacknowledged I/O requests when SQUID stops opening new files. If this many messages are in the queues, SQUID won't open new files. Default is 64 Q2 specifies the number of unacknowledged messages when SQUID starts blocking. If this many messages are in the queues, SQUID blocks until it receives some replies. Default is 72 The coss store type:

block-size=n defines the "block size" for COSS cache_dir's. SQUID uses file numbers as block numbers. Since file numbers are limited to 24 bits, the block size determines the maximum size of the COSS partition. The default is 512 bytes, which leads to a maximum cache_dir size of $512 \ll 24$, or 8 GB. Note that you should not change the coss block size after SQUID has written some objects to the cache_dir.

Common options:

read-only, this cache_dir is read only.

max-size=n, refers to the max object size this storedir supports. It is used to initially choose the storedir to dump the object. Note: To make optimal use of the max-size limits you should order the cache_dir lines with the smallest max-size value first and the ones with no max-size specification last.

Note that for coss, max-size must be less than COSS_MEMBUF_SZ (hard coded at 1 MB).

cache_access_log

Logs the client request activity. Contains an entry for every HTTP and ICP queries received. To disable, enter "none".

cache_log

Cache logging file. This is where general information about your cache's behavior goes. You can increase the amount of data logged to this file with the "debug_options" tag below.

cache_store_log

Logs the activities of the storage manager. Shows which objects are ejected from the cache, and which objects are saved and for how long. To disable, enter "none". There are not really utilities to analyze this data, so you can safely disable it.

cache_swap_log

Location for the cache "swap.log." This log file holds the metadata of objects saved on disk. It is used to rebuild the cache during startup. Normally this file resides in each 'cache_dir' directory, but you may specify an alternate pathname here. Note you must give a full filename, not just a directory. Since this is the index for the whole object list you CANNOT periodically rotate it!

If %s can be used in the file name then it will be replaced with a representation of the cache_dir name where each / is replaced with '.'. This is needed to allow adding/removing cache_dir lines when cache_swap_log is being used. If have more than one 'cache_dir', and %s is not used in the name then these swap logs will have names such as:

```
cache_swap_log.00  
cache_swap_log.01  
cache_swap_log.02
```

The numbered extension (which is added automatically) corresponds to the order of the 'cache_dir' lines in this configuration file. If you change the order of the 'cache_dir' lines in this file, then these log files will NOT correspond to the correct 'cache_dir' entry (unless you manually rename them). We recommend that you do NOT use this option. It is better to keep these log files in each 'cache_dir' directory.

emulate_httpd_log on|off

The Cache can emulate the log file format which many 'httpd' programs use. To disable/enable this emulation, set emulate_httpd_log to 'off' or 'on'. The default is to use the native log format since it includes useful information that SQUID-specific log analyzers use.

log_ip_on_direct on|off

Log the destination IP address in the hierarchy log tag when going direct. Earlier SQUID versions logged the hostname here. If you prefer the old way set this to off.

mime_table

Pathname to SQUID's MIME table. You shouldn't need to change this, but the default file contains examples and formatting information if you do.

log_mime_hdrs on|off

The Cache can record both the request and the response MIME headers for each HTTP transaction. The headers are encoded safely and will appear as two bracketed fields at the end of the access log (for either the native or httpd-emulated log formats). To enable this logging set log_mime_hdrs to 'on'.

useragent_log

SQUID will write the User-Agent field from HTTP requests to the filename specified here. By default useragent_log is disabled.

referer_log

SQUID will write the Referer field from HTTP requests to the filename specified here. By default referer_log is disabled.

pid_filename

A filename to write the process-id to. To disable, enter "none".

debug_options

Logging options are set as section,level where each source file is assigned a unique section. Lower levels result in less output, Full debugging (level 9) can result in a very large log file, so be careful. The magic word "ALL" sets debugging levels for all sections. We recommend normally running with "ALL,1".

log_fqdn on|off

Turn this on if you wish to log fully qualified domain names in the access.log. To do this SQUID does a DNS lookup of all IP's connecting to it. This can (in some situations) increase latency, which makes your cache seem slower for interactive browsing.

client_netmask

A netmask for client addresses in logfiles and cachemgr output. Change this to protect the privacy of your cache clients. A netmask of 255.255.255.0 will log all IP's in that range with the last digit set to '0'.

Options for Tuning the Cache**wais_relay_host****wais_relay_port**

Relay WAIS request to host (1st arg) at port (2 arg).

request_header_max_size (KB)

This specifies the maximum size for HTTP headers in a request. Request headers are usually relatively small (about 512 bytes). Placing a limit on the request header size will catch certain bugs (for example with persistent connections) and possibly buffer-overflow or denial-of-service attacks.

request_body_max_size (KB)

This specifies the maximum size for an HTTP request body. In other words, the maximum size of a PUT/POST request. A user who attempts to send a request with a body larger than this limit receives an "Invalid Request" error message. If you set this parameter to a zero (the default), there will be no limit imposed.

refresh_pattern

usage: refresh_pattern [-i] regex min percent max [options]

By default, regular expressions are CASE-SENSITIVE. To makethem case-insensitive, use the -i option.

'Min' is the time (in minutes) an object without an explicit expiry time should be considered fresh. The recommended value is 0, any higher values may cause dynamic applications to be erroneously cached unless the application designer has taken the appropriate actions.

'Percent' is a percentage of the objects age (time since last modification age) an object without explicit expiry time will be considered fresh.

'Max' is an upper limit on how long objects without an explicit expiry time will be considered fresh. options: override-expire, override-lastmod, reload-into-ims, ignore-reload.

override-expire enforces min age even if the server sent a Expires: header. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

override-lastmod enforces min age even on objects that was modified recently.

reload-into-ims changes client no-cache or ``reload" to If-Modified-Since requests. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

ignore-reload ignores a client no-cache or ``reload" header. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

Basically a cached object is:

```
FRESH if expires < now, else STALE
STALE if age > max
FRESH if lm-factor < percent, else STALE
FRESH if age < min
else STALE
```

The refresh_pattern lines are checked in the order listed here. The first entry which matches is used. If none of the entries match, then the default will be used.

Note, you must uncomment all the default lines if you want to change one. The default setting is only active if none is used.

Suggested default:

refresh_pattern ^ftp:	1440	20%	10080
refresh_pattern ^gopher:	1440	0%	1440
refresh_pattern .	0	20%	4320

quick_abort_min	(KB)
quick_abort_max	(KB)
quick_abort_pct	(percent)

The cache by default continues downloading aborted requests which are almost completed (less than 16 KB remaining). This may be undesirable on slow (e.g. SLIP) links and/or very busy caches. Impatient users may tie up file descriptors and bandwidth by repeatedly requesting and immediately aborting downloads.

When the user aborts a request, SQUID will check the quick_abort values to the amount of data transfered until then.

If the transfer has less than 'quick_abort_min' KB remaining, it will finish the retrieval.

If the transfer has more than 'quick_abort_max' KB remaining, it will abort the retrieval.

If more than 'quick_abort_pct' of the transfer has completed, it will finish the retrieval.

If you do not want any retrieval to continue after the client has aborted, set both 'quick_abort_min' and 'quick_abort_max' to '0 KB'.

If you want retrievals to always continue if they are being cached then set 'quick_abort_min' to '-1 KB'.

negative_ttl time-units
Time-to-Live (TTL) for failed requests. Certain types of failures (such as "connection refused" and "404 Not Found") are negatively-cached for a configurable amount of time. The default is 5 minutes. Note that this is different from negative caching of DNS lookups.

positive_dns_ttl time-units
Time-to-Live (TTL) for positive caching of successful DNS lookups. Default is 6 hours (360 minutes). If you want to minimize the use of SQUID's ipcache, set this to 1, not 0.

negative_dns_ttl time-units
Time-to-Live (TTL) for negative caching of failed DNS lookups.

range_offset_limit (bytes)
Sets a upper limit on how far into the the file a Range request may be to cause SQUID to prefetch the whole file. If beyond this limit then SQUID forwards the Range request as it is and the result is NOT cached.

This is to stop a far ahead range request (lets say start at 17MB) from making SQUID fetch the whole object up to that point before sending anything to the client.

A value of -1 causes SQUID to always fetch the object from the beginning so that it may cache the result. (2.0 style)

A value of 0 causes SQUID to never fetch more than the client requested. (default)

Timeout Values

connect_timeout time-units

Some systems (notably Linux) can not be relied upon to properly time out connect(2) requests. Therefore the SQUID process enforces its own timeout on server connections. This parameter specifies how long to wait for the connect to complete. The default is two minutes (120 seconds).

peer_connect_timeout time-units

This parameter specifies how long to wait for a pending TCP connection to a peer cache. The default is 30 seconds. You may also set different timeout values for individual neighbors with the 'connect-timeout' option on a 'cache_peer' line.

read_timeout time-units

The read_timeout is applied on server-side connections. After each successful read(), the timeout will be extended by this amount. If no data is read again after this amount of time, the request is aborted and logged with ERR_READ_TIMEOUT. The default is 15 minutes.

request_timeout

How long to wait for an HTTP request after initial connection establishment.

persistent_request_timeout

How long to wait for the next HTTP request on a persistent connection after the previous request completes.

client_lifetime time-units

The maximum amount of time that a client (browser) is allowed to remain connected to the cache process. This protects the Cache from having a lot of sockets (and hence file descriptors) tied up in a CLOSE_WAIT state from remote clients that go away without properly shutting down (either because of a network failure or because of a poor client implementation). The default is one day, 1440 minutes.

NOTE: The default value is intended to be much larger than any client would ever need to be connected to your cache. You should probably change client_lifetime only as a last resort. If you seem to have many client connections tying up filedescriptors, we recommend first tuning the read_timeout, request_timeout, persistent_request_timeout and quick_abort values.

half_closed_clients

Some clients may shutdown the sending side of their TCP connections, while leaving their receiving sides open. Sometimes, SQUID can not tell the difference between a half-closed and a fully-closed TCP connection. By default, half-closed client connections are kept open until a read(2) or write(2) on the socket returns an error.

Change this option to 'off' and SQUID will immediately close client connections when read(2) returns

"no more data to read."

pconn_timeout

Timeout for idle persistent connections to servers and other proxies.

ident_timeout

Maximum time to wait for IDENT lookups to complete.

If this is too high, and you enabled IDENT lookups from untrusted users, then you might be susceptible to denial-of-service by having many ident requests going at once.

shutdown_lifetime time-units

When SIGTERM or SIGHUP is received, the cache is put into "shutdown pending" mode until all active sockets are closed. This value is the lifetime to set for all open descriptors during shutdown mode. Any active clients after this many seconds will receive a 'timeout' message.

Administrative Parameters

cache_mgr

Email-address of local cache manager who will receive mail if the cache dies. The default is "webmaster."

cache_effective_user

cache_effective_group

If the cache is run as root, it will change its effective/real UID/GID to the UID/GID specified below. The default is to change to UID to nobody and GID to the default group of nobody.

If SQUID is not started as root, the default is to keep the current UID/GID, and only the GID can be changed to any of the groups the user starting SQUID is member of. Note that if SQUID is not started as root then you cannot set http_port to a value lower than 1024.

visible_hostname

If you want to present a special hostname in error messages, etc, then define this. Otherwise, the return value of gethostname() will be used. If you have multiple caches in a cluster and get errors about IP-forwarding you must set them to have individual names with this setting.

unique_hostname

If you want to have multiple machines with the same 'visible_hostname' then you must give each machine a different 'unique_hostname' so that forwarding loops can be detected.

hostname_aliases

A list of other DNS names that your cache has.

Options for the Cache Registration Service

This section contains parameters for the (optional) cache announcement service. This service is provided to help cache administrators locate one another in order to join or create cache hierarchies.

An 'announcement' message is sent (via UDP) to the registration service by SQUID. By default, the announcement message is NOT SENT unless you enable it with 'announce_period' below.

The announcement message includes your hostname, plus the following information from this configuration file:

```
http_port
icp_port
cache_mgr
```

All current information is processed regularly and made available on the Web at <http://www.ircache.net/Cache/Tracker/>.

announce_period

This is how frequently to send cache announcements. The default is '0' which disables sending the announcement messages.

To enable announcing your cache, just uncomment the line below.

To enable announcing your cache, just uncomment the line below.
announce_period 1 day

announce_host

announce_file

announce_port

announce_host and **announce_port** set the hostname and port number where the registration message will be sent.

Hostname will default to 'tracker.ircache.net' and port will default default to 3131. If the 'filename' argument is given, the contents of that file will be included in the announce message.

Miscellaneous

dns_testnames

The DNS tests exit as soon as the first site is successfully looked up

This test can be disabled with the -D command line option.

logfile_rotate

Specifies the number of logfile rotations to make when you type 'SQUID -k rotate'. The default is 10, which will rotate with extensions 0 through 9. Setting logfile_rotate to 0 will disable the rotation, but the logfiles are still closed and re-opened. This will enable you to rename the logfiles yourself just before sending the rotate signal.

Note, the 'SQUID -k rotate' command normally sends a USR1 signal to the running SQUID process. In certain situations (e.g. on Linux with Async I/O), USR1 is used for other purposes, so -k rotate uses another signal. It is best to get in the habit of using 'SQUID -k rotate' instead of 'kill -USR1 <pid>'.

append_domain

Appends local domain name to hostnames without any dots in them. append_domain must begin with a period.

Be warned that there today is Internet names with no dots in them using only top-domain names, so setting this may cause some Internet sites to become unavailable.

tcp_recv_bufsize (bytes)

Size of receive buffer to set for TCP sockets. Probably just as easy to change your kernel's default. Set to zero to use the default buffer size.

err_html_text

HTML text to include in error messages. Make this a "mailto" URL to your admin address, or maybe just a link to your organizations Web page.

To include this in your error messages, you must rewrite the error template files (found in the "errors" directory). Wherever you want the 'err_html_text' line to appear, insert a %L tag in the error template file.

deny_info

Usage: deny_info err_page_name acl
or deny_info http://... acl

Example: deny_info ERR_CUSTOM_ACCESS_DENIED bad_guys

This can be used to return a ERR_page for requests which do not pass the 'http_access' rules. A single ACL will cause the http_access check to fail. If a 'deny_info' line exists for that ACL then SQUID returns a corresponding error page.

You may use ERR_pages that come with SQUID or create your own pages and put them into the configured errors/ directory.

Alternatively you can specify an error URL. The browsers will then get redirected (302) to the specified URL. %s in the redirection URL will be replaced by the requested URL.

Alternatively you can tell SQUID to reset the TCP connection by specifying TCP_RESET.

memory_pools on|off

If set, SQUID will keep pools of allocated (but unused) memory available for future use. If memory is a premium on your system and you believe your malloc library outperforms SQUID routines, disable this.

memory_pools_limit (bytes)

Used only with memory_pools on:

memory_pools_limit 50 MB

If set to a non-zero value, SQUID will keep at most the specified limit of allocated (but unused) memory in memory pools. All free() requests that exceed this limit will be handled by your malloc library. SQUID does not pre-allocate any memory, just safe-keeps objects that otherwise would be free()d. Thus, it is safe to set memory_pools_limit to a reasonably high value even if your configuration will use less memory.

If not set (default) or set to zero, SQUID will keep all memory it can. That is, there will be no limit on the total amount of memory used for safe-keeping.

To disable memory allocation optimization, do not set memory_pools_limit to 0. Set memory_pools to "off" instead.

An overhead for maintaining memory pools is not taken into account when the limit is checked. This overhead is close to four bytes per object kept. However, pools may actually _save_ memory because of reduced memory thrashing in your malloc library.

forwarded_for on|off

If set, SQUID will include your system's IP address or name in the HTTP requests it forwards. By default it looks like this:

X-Forwarded-For: 192.1.2.3

If you disable this, it will appear as

X-Forwarded-For: unknown

log_icp_queries on|off

If set, ICP queries are logged to access.log. You may wish to disable this if your ICP load is VERY high to speed things up or to simplify log analysis.

icp_hit_stale on|off

If you want to return ICP_HIT for stale cache objects, set this option to 'on'. If you have sibling relationships with caches in other administrative domains, this should be 'off'. If you only have sibling relationships with caches under your control, then it is probably okay to set this to 'on'.

If set to 'on', then your siblings should use the option "allow-miss" on their cache_peer lines for connecting to you.

minimum_direct_hops

If using the ICMP pinging stuff, do direct fetches for sites which are no more than this many hops away.

minimum_direct_rtt

If using the ICMP pinging stuff, do direct fetches for sites which are no more than this many rtt milliseconds away.

cachemgr_passwd

Specify passwords for cachemgr operations.

Usage: cachemgr_passwd password action action ...

Some valid actions are (see cache manager menu for a full list):

- 5min
- 60min
- asndb
- authenticator
- cbdata
- client_list
- comm_incoming
- config *
- counters
- delay
- digest_stats
- dns
- events
- filedescriptors
- fqdnocache
- histograms
- http_headers
- info
- io
- ipcache
- mem
- menu
- netdb
- non_peers
- objects
- offline_toggle *
- pconn
- peer_select
- redirector
- refresh
- server_list
- shutdown *
- store_digest
- storedir
- utilization
- via_headers
- vm_objects

* Indicates actions which will not be performed without a valid password, others can be performed if not listed here.

To disable an action, set the password to "disable". To allow performing an action without a password, set the password to "none".

Use the keyword "all" to set the same password for all actions.

Example:

```
cachemgr_passwd secret shutdown
cachemgr_passwd lesssssssecret info stats/objects
cachemgr_passwd disable all
```

store_avg_object_size (kbytes)

Average object size, used to estimate number of objects your cache can hold. See doc/Release-Notes-1.1.txt. The default is 13 KB.

store_objects_per_bucket

Target number of objects per bucket in the store hash table. Lowering this value increases the total number of buckets and also the storage maintenance rate. The default is 50.

client_db on|off

If you want to disable collecting per-client statistics, then turn off client_db here.

netdb_low

netdb_high

The low and high water marks for the ICMP measurement database. These are counts, not percents. The defaults are 900 and 1000. When the high water mark is reached, database entries will be deleted until the low mark is reached.

netdb_ping_period

The minimum period for measuring a site. There will be at least this much delay between successive pings to the same network. The default is five minutes.

query_icmp on|off

If you want to ask your peers to include ICMP data in their ICP replies, enable this option.

If your peer has configured SQUID (during compilation) with '--enable-icmp' then that peer will send ICMP pings to origin server sites of the URLs it receives. If you enable this option then the ICP replies from that peer will include the ICMP data (if available). Then, when choosing a parent cache, SQUID will choose the parent with the minimal RTT to the origin server. When this happens, the hierarchy field of the access.log will be "CLOSEST_PARENT_MISS". This option is off by default.

test_reachability on|off

When this is 'on', ICP MISS replies will be ICP_MISS_NOFETCH instead of ICP_MISS if the target host is NOT in the ICMP database, or has a zero RTT.

buffered_logs on|off

cache.log log file is written with stdio functions, and as such it can be buffered or unbuffered. By default it will be unbuffered. Buffering it can speed up the writing slightly (though you are unlikely to need to worry unless you run with tons of debugging enabled in which case performance will suffer badly anyway..).

reload_into_ims on|off

When you enable this option, client no-cache or ``reload" requests will be changed to If-Modified-Since requests. Doing this VIOLATES the HTTP standard. Enabling this

feature could make you liable for problems which it causes.

see also `refresh_pattern` for a more selective approach.

always_direct

Usage: `always_direct allow|deny [!]aclname ...`

Here you can use ACL elements to specify requests which should ALWAYS be forwarded directly to origin servers. For example, to always directly forward requests for local servers use something like:

```
acl local-servers dstdomain my.domain.net
always_direct allow local-servers
```

To always forward FTP requests directly, use

```
acl FTP proto FTP
always_direct allow FTP
```

NOTE: There is a similar, but opposite option named 'never_direct'. You need to be aware that "always_direct deny foo" is NOT the same thing as "never_direct allow foo". You may need to use a deny rule to exclude a more-specific case of some other rule. Example:

```
acl local-external dstdomain external.foo.net
acl local-servers dstdomain .foo.net
always_direct deny local-external
always_direct allow local-servers
```

This option replaces some v1.1 options such as `local_domain` and `local_ip`.

never_direct

Usage: `never_direct allow|deny [!]aclname ...`

`never_direct` is the opposite of `always_direct`. Please read the description for `always_direct` if you have not already.

With 'never_direct' you can use ACL elements to specify requests which should NEVER be forwarded directly to origin servers. For example, to force the use of a proxy for all requests, except those in your local domain use something like:

```
acl local-servers dstdomain .foo.net
acl all src 0.0.0.0/0.0.0.0
never_direct deny local-servers
never_direct allow all
```

or if SQUID is inside a firewall and there is local intranet servers inside the firewall then use something like:

```
acl local-intranet dstdomain .foo.net
acl local-external dstdomain external.foo.net
always_direct deny local-external
always_direct allow local-intranet
never_direct allow all
```

This option replaces some v1.1 options such as `inside_firewall` and `firewall_ip`.

header_access

Usage: `header_access header_name allow|deny [!]aclname ...`

WARNING: Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

This option replaces the old 'anonymize_headers' and the older 'http_anonymizer' option with something that is much more configurable. This new method creates a list of ACLs for each header, allowing you very fine-tuned header mangling.

You can only specify known headers for the header name. Other headers are reclassified as 'Other'. You can also refer to all the headers with 'All'.

For example, to achieve the same behaviour as the old 'http_anonymizer standard' option, you should use:

```
header_access From deny all
header_access Referer deny all
header_access Server deny all
header_access User-Agent deny all
header_access WWW-Authenticate deny all
header_access Link deny all
```

Or, to reproduce the old 'http_anonymizer paranoid' feature you should use:

```
header_access Allow allow all
header_access Authorization allow all
header_access WWW-Authenticate allow all
header_access Cache-Control allow all
header_access Content-Encoding allow all
header_access Content-Length allow all
header_access Content-Type allow all
header_access Date allow all
header_access Expires allow all
header_access Host allow all
```

header_access If-Modified-Since allow all
header_access Last-Modified allow all
header_access Location allow all
header_access Pragma allow all
header_access Accept allow all
header_access Accept-Charset allow all
header_access Accept-Encoding allow all
header_access Accept-Language allow all
header_access Content-Language allow all
header_access Mime-Version allow all
header_access Retry-After allow all
header_access Title allow all
header_access Connection allow all
header_access Proxy-Connection allow all
header_access All deny all

By default, all headers are allowed (no anonymizing is performed).

header_replace

Usage: header_replace header_name message
Example: header_replace User-Agent Nutscape/1.0 (CP/M; 8-bit)

This option allows you to change the contents of headers denied with header_access above, by replacing them with some fixed string. This replaces the old fake_user_agent option.

By default, headers are removed if denied.

icon_directory

Where the icons are stored. These are normally kept in c:/SQUID/share/icons

error_directory

If you wish to create your own versions of the default (English) error files, either to customize them to suit your language or company copy the template English files to another directory and point this tag at them.

maximum_single_addr_tries

This sets the maximum number of connection attempts for a host that only has one address (for multiple-address hosts, each address is tried once).

The default value is three tries, the (not recommended) maximum is 255 tries. A warning message will be generated if it is set to a value greater than ten.

snmp_port

SQUID can now serve statistics and status information via SNMP. By default it listens to port 3401 on the machine. If you don't wish to use SNMP, set this to "0".

snmp_access

Allowing or denying access to the SNMP port.

All access to the agent is denied by default.

usage:

```
snmp_access allow|deny [!]aclname ...
```

Example:

```
snmp_access allow snmppublic localhost
snmp_access deny all
```

snmp_incoming_address

snmp_outgoing_address

Just like 'udp_incoming_address' above, but for the SNMP port.

snmp_incoming_address is used for the SNMP socket receiving messages from SNMP agents.

snmp_outgoing_address is used for SNMP packets returned to SNMPagents.

The default snmp_incoming_address (0.0.0.0) is to listen on all available network interfaces.

If snmp_outgoing_address is set to 255.255.255.255 (the default) then it will use the same socket as snmp_incoming_address. Only change this if you want to have SNMP replies sent using another address than where this SQUID listens for SNMP queries.

NOTE, snmp_incoming_address and snmp_outgoing_address can not have the same value since they both use port 3401.

as_whois_server

WHOIS server to query for AS numbers. NOTE: AS numbers are queried only when SQUID starts up, not for every request.

MIME Type Configuration Options

The MIME.CONF file associates filename extensions (for servers or services that don't automatically include them – like FTP) with a mime type and a graphical icon. Content-Encoding names are taken directly from section 3.1 of RFC2068 (HTTP/1.1)

This file has the following format information on each line:

RegEx mode	Content-type	icon name	content-encoding	transfer-
-------------------	---------------------	------------------	-------------------------	------------------

Here are a couple of examples from the default file:

\.bin\$	application/macbinary	anthony-unknown.gif	-image	
\.exe\$	application/octet-stream	anthony-unknown.gif	-image	
\.pdf\$	application/pdf	anthony-unknown.gif	-	

It is unlikely that you will wish to modify the default MIME encoding that come in the shipped version of this product.

Cache Testing and Troubleshooting

Testing your PatchLink Distribution Point content caching solution

Setup 1: Deploy the PatchLink Distribution Point package to designated local patch storage server.

When deployed the package be will auto configured:

- a) Setup cache folders
- b) Configured to utilize port 25253

Setup 2: Verify that the Cache Server is Caching.

- 1. Point your web browser at the cache-ip (192.168.3.59 in Patchlink lab environment) and port 25253
- 2. Surf the web -- make sure you have no problems going thru the cache and hitting www.cnn.com, www.southcitygrill.com, etc.
- 3. Allow anonymous access to the updatestorage folder with directory browsing enabled via IIS
- 4. Browse to this location and right click "save as" on a few patches...do the same one twice
- 5. Check the c:\program files\patchlink\distribution point\var\logs directory and view the access.log, there will be TCP_HIT and TCP_MISS status lines:
 - a. MISS <--- file not in cache
 - b. HTTP_HIT <--- file pulled locally and not from upstream wire

Step Three: If all that works... test the agent...

- 1. Set the agent via control panel to use cache-ip address (192.168.3.59 in Patchlink lab environment) and the port 25253
- 2. Log into plus server – (192.168.3.8 in Patchlink lab environment), and set the server's communication interval, under options, to 1 minute
- 3. Watch the log, (about 3 lines every 1 minute)... communication is working
- 4. Deploy the "A - Deployment Test and Diagnostic Package" to the agent
- 5. Watch the access.log file "AND" the local \windows\temp or \WINNT\temp directory for a text file to appear.
- 6. You should see a GET request in the LOG with a TCP-MISS
- 7. Deploy the same patch... watch the log
- 8. You should see a TCP_MEM_HIT <<< it's only a 1k file... it's a memory cached hit...
- 9. You can deploy any other patch and when you get to the additional flags field add -pldo (-pldo means just move the patch to the temp dir but don't execute)
- 10. Verify by watching access.log and looking at the temp dir for a .exe file or text file
- 11. Delete the file in temp dir.
- 12. Redo deployment... look for a TCP_HIT in the access.log

To remove the PatchLink Distribution Point server from the installed server:

```
Cd c:\program files\patchlink\distribution point\sbin
squid.exe -n patchlink_distribution -r
```

Troubleshooting

```
CD c:\program files\patchlink\distribution point\sbin
```

Execute the following to create the cache directories and get things set up:

```
squid.exe -f c:/progra~1/patchli~1/distrib~1/etc/squid.conf -z
```

Check to see if there are any errors in the Event Log.

Execute the following to manually run the PatchLink Distribution Point application:

```
squid.exe -f c:/progra~1/patchli~1/distrib~1/etc/squid.conf
```

Look in c:\program files\patchlink\distribution point\VAR\CACHE.LOG if the Squid process dies. See what it says if there are any other mis-configurations.

Fix any mis-configurations or problems and retry these Trouble shooting steps.

Other supported operating systems

Linux agent versions

PatchLink supports several distributions of Red Hat Linux including:

- 7.0, 7.1, 7.2, 7.3
- 8.0
- 9.0

The Linux agent requires the Java Runtime Environment (JRE) v1.2.2 or above, and can only be installed in single agent mode.

UNIX versions

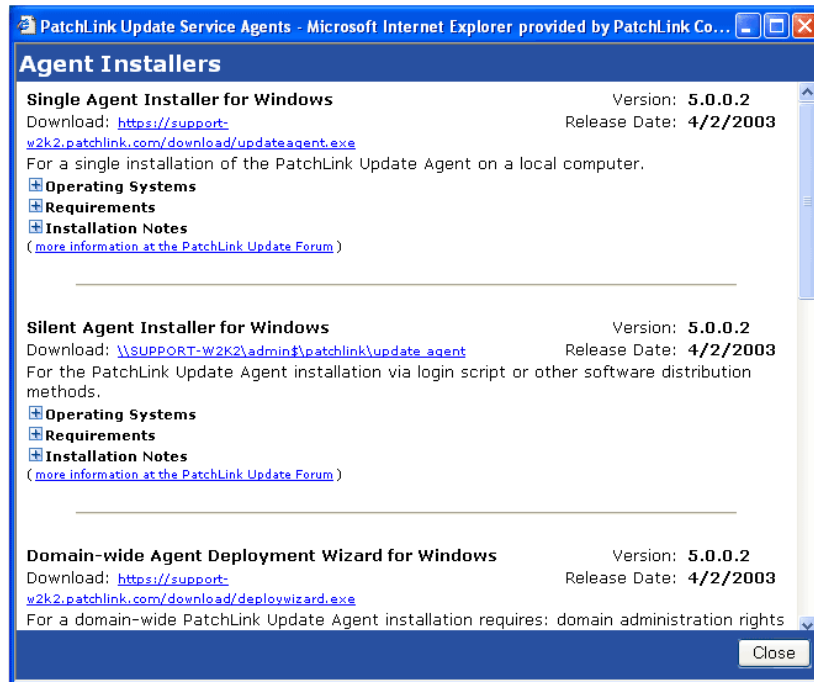
Like Linux, the UNIX requires JRE v1.2.2 and above. The following operation systems are supported:

- Solaris
- v2.5, v2.6, v 2.7, v7, and v8

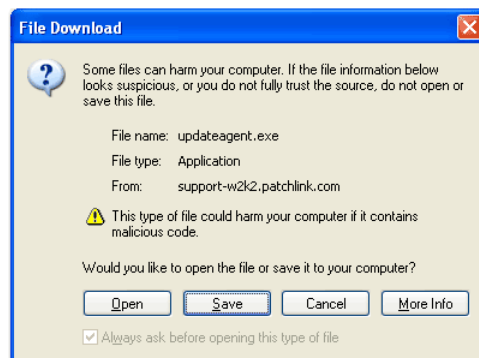
Single Agent

The Single Agent Installer is used to manually add a single computer to the managed computers list. This is most often used in the case of stand alone computers.

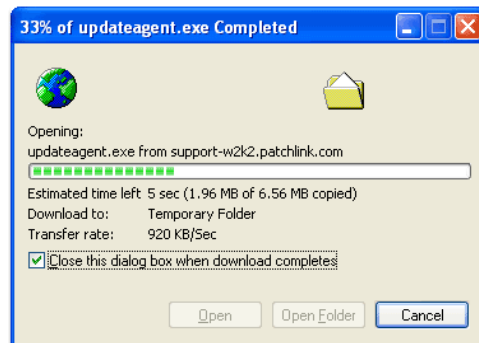
The agent installer screen contains links to all of the agent installations and additional information on Operating Systems, Requirements, and Installation Notes.



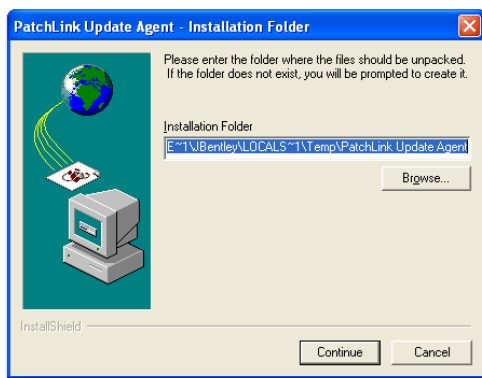
- Select the Single Agent Installer for Windows link.



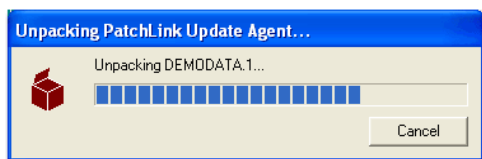
- Click on the **Open** button



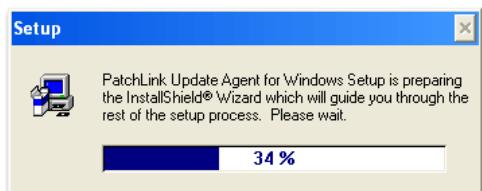
- Select the destination directory for the installation files, and click on the **Continue**.



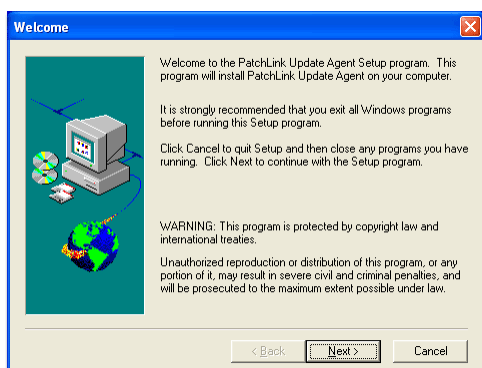
- Files Unpack



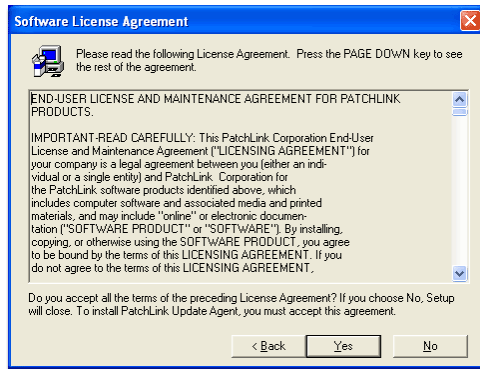
- Files Setup



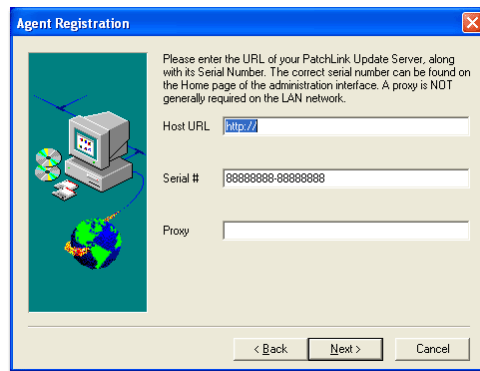
- Read the Welcome screen and click **Next** to continue.



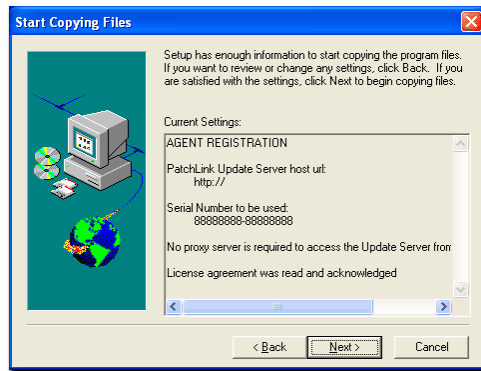
- Read the license agreement, and click “Yes” to continue



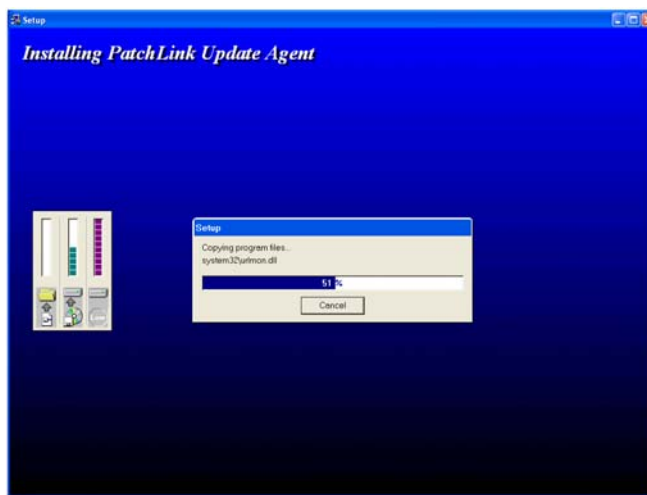
- Enter the “Host URL”, “Serial #”, and “Proxy” server address, then click “Next” to continue.



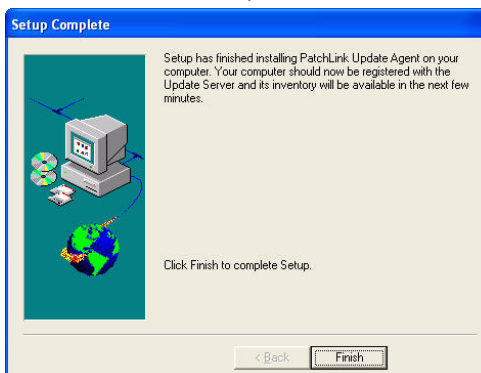
- Confirm the installation settings, and click “Next” to continue.



- Patchlink Update Agent Installs.



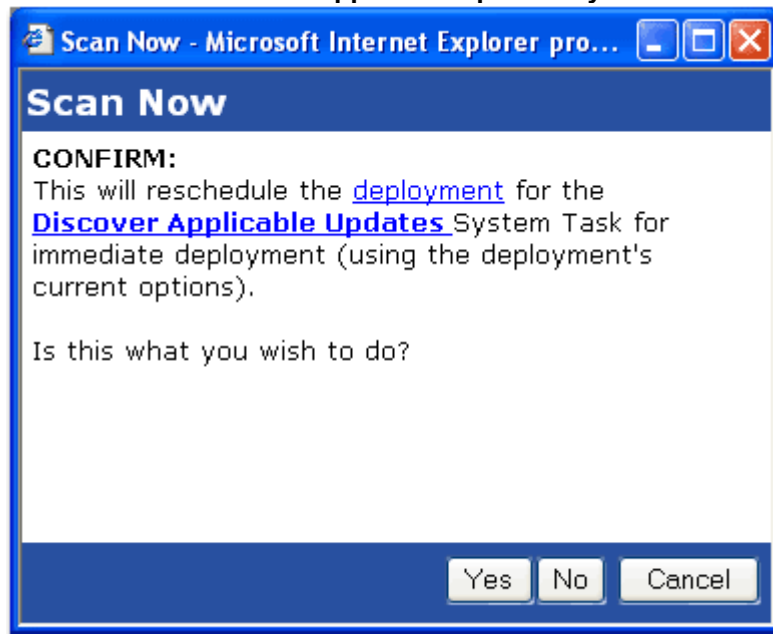
- Click **Finish** to complete the installation



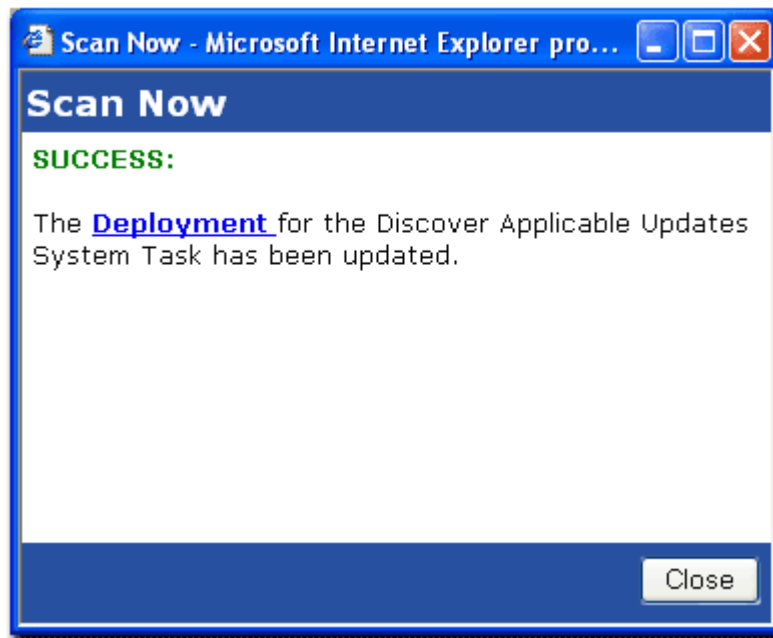
- **View**
To display additional information about the computer, select a computer and click on the View button. This performs the same function as clicking on the name of the computer.
- **Enable**
To enable selected disabled computers, click on the Enable button.
- **Disable**
To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.
- **Export**
Export the computer list data to a comma-separated value (CSV) file. The filter and order of the data is based on what the Computer List view is selected and sorted on. This may display only a certain number of computers per page, the export will save all computer data based on your selected filter.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected computers.

To initialize (choose) all computers, click the **Scan Now** button without selecting any computers.

If you choose not to select any computers, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the computers.



To reschedule the **Discover Applicable Updates**, select Yes.



PLUS will reschedule the selected computer(s)'s membership (or all computers' memberships), initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

10.5 Computers Security

The [Computer List](#) section of PLUS requires the [View Computers](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to be able display the agent installers' page requires the [Install Computers](#) access right. If a user does not have the correct access, the [Install](#) button is displayed. Once a computer registers against PLUS a PatchLink Administrator must give access to that computer to other user security roles.

To be able to enable, disable, and remove computers requires the [Manage Computers](#) access right. If a user does not have the correct access, the [Enable](#), [Disable](#), and [Remove](#) buttons are disabled.

To export the computer data to a comma-separated value (CSV) file requires the [Export Computer Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

To restart the discovery and analysis process for all of the computers registered to the PLUS requires the [Manage System Tasks](#) access right. If a user does not have the correct access, the [Scan Now](#) button is disabled.

Contact your PatchLink Administrator for more information on [PatchLink Update Security](#).

10.6 Computer Details

The Computer Details section of PLUS displays PLUS related and important information about a specific computer. Click on the actual Computer Name link under the Computer Name column. This will bring you to the details page.

- Selecting the Vulnerabilities tab will display the Vulnerability Analysis for the computer.
- Selecting Inventory tab will display the Inventory for the computer.
- Selecting Deployments tab will display the deployments for the computer.

The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. [See Section 5; Vulnerabilities](#), [Section 6; Inventory](#), and [Section 7; Packages](#) for more detailed information.

Information	Reports	Inventory	Deployments
Computer Information:			
Name: \\CRAP-TOP		Description: Rene's Lap Top	
Operating System: WinXP		OS Version: 5.1	
OS Service Pack: Service Pack 1		OS Build Number: 2600	
DNS Name: crap-top		IP Address: 192.168.1.218	
Agent Information:			
PLUS Agent Installation Date: 6/20/2003 3:35:07 PM (GMT-07:00)		PLUS Agent Status: Offline	
PLUS Agent Version: 5.0.0.2		Last Connected Date: 7/11/2003 5:46:21 PM (GMT-07:00)	
Group Information:			
Group Name	Type	Status	Added By
WinXP	Computer (system created)	Enabled	PatchLink Corp.
Added On		6/10/2003 9:26:54 AM (GMT-07:00)	
Policy Information:			
Communication Interval	Hours of Operation	Logging Level	
2 Minutes	Always Run	Basic Info	

If information is not applicable to a specific section, the section will simply not be present on the details page.

- Computer Information
 - Name: This displays the name of the computer
 - Operating System: This displays the abbreviated operating system platform name of the computer.
 - OS Service Pack: This displays the service pack level of the computer
 - DNS Name: This displays the DNS name of the computer.
 - Description: This displays the description of the computer.
 - OS Version: This displays the operating system version number of the computer.
 - OS Build Number: This displays the operating system build number of the computer.
 - IP Address: This displays the IP Address of the computer.

- Agent Information
 - PLUS Agent Installation Date: The date the agent was installed and registered against PLUS.
 - PLUS Agent Version: This displays the version of the agent.
 - PLUS Agent Status: This displays the status of the agent.
 - Last Connected Date: The date the agent last contacted PLUS.
- Group Information
 - Group Name: This displays the name of the group the computer is a member of.
 - Type: This displays the type of the group.
 - Status: This displays the status of the group.
 - Added By: This displays the PatchLink User who added the computer to the group.
 - Added On: This displays the date the computer was added to the group.
- Policy Information
 - Communication Level: This displays how often the agent communicates with PLUS.
 - Hours of Operation: This displays the hours of operation in which the agent will communicate with PLUS.
 - Logging Level: The logging level determines how much data the agent will log while it performs its tasks.

10.7 Page Functions

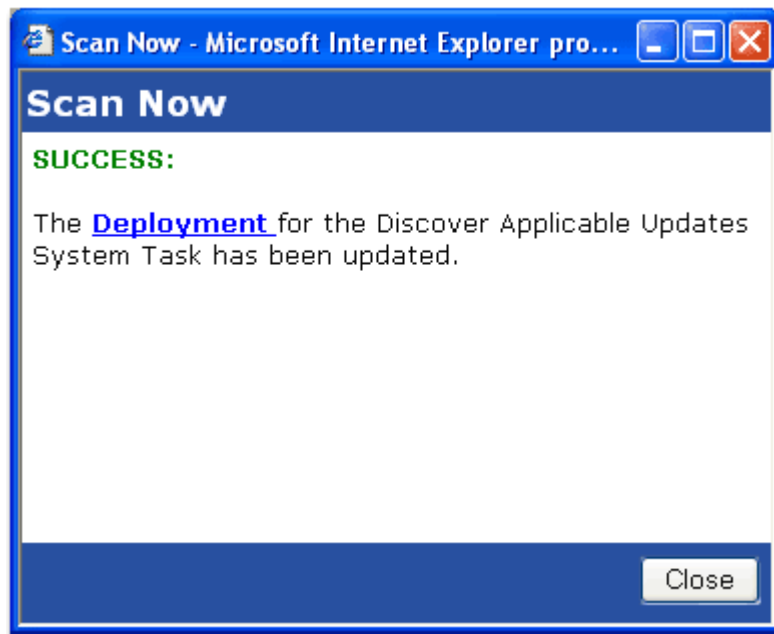
- Vulnerabilities Tab
Selecting this tab will display the Vulnerability Analysis for the computer.
- Inventory Tab
Selecting this tab will display the Inventory for the computer.
- Deployments Tab
Selecting this tab will display the deployments for the computer.

10.8 Action Menu



- **Export**
Export the computer information to a comma-separated value (CSV) file.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected computers.

PLUS will reschedule the computer and initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.



Upon clicking the Close button on the screen, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

10.9 Computer Details Security

The [Computer Information](#) section of PLUS requires the [View Computers](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To export the computer information to a comma-separated value (CSV) file requires the [Export Computer Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

To restart the discovery and analysis process for all of the computers registered to the PLUS requires the [Manage System Tasks](#) access right. If a user does not have the correct access, the [Scan Now](#) button is disabled.

To be able to view the vulnerability results for the computer requires the [View Vulnerabilities](#) access right. If a user does not have the correct access, the [Vulnerabilities](#) tab is disabled.

To be able to view the computer inventory section requires the [View OS Inventories](#) access right. If a user does not have the correct access, the [Inventory](#) tab is disabled.

To be able to view the computer deployments section requires the [View Deployment Status](#) access right. If a user does not have the correct access, the [Deployments](#) tab is disabled.

Contact your PatchLink Administrator for more information on [PatchLink Update Security](#).

10.10 Vulnerabilities by Computer

A Vulnerability consists of the vulnerability description, the signatures and fingerprints required to determine whether the vulnerability is patched or not patched, and the associated package or packages for performing the patch.

Click on the **Vulnerabilities tab** in the Computer Details screen.

Computers

Home | Reports | Inventory | Packages | **Computers** | Groups | Users | Options | Help |

Server Time: 7/17/2003 2:30:07 PM (GMT-07:00)

Vulnerability Reports by Computer: \\CITIDAL

Filter By: Detected

Information **Report Analysis** Inventory Deployments

Total: 63

Report Name	Impact	✓	✗	⚙	🔄	📄	🔍
A - Deployment Test and Diagnostic Package	Critical	1	0	0	0	1	100%
AA - Update Agent Hotfix 5.0 for Windows Rene G	Critical	0	1	0	0	1	100%
A-Detect for pctspk.exe	Critical	0	1	0	0	1	100%
Amruta Break Agent	Critical	0	1	0	0	1	100%
C - PatchLink Update Agent Hotfix 4.00.06 --MUST INSTALL--	Critical	1	0	0	0	1	100%
C - PatchLink Update Agent Hotfix 4.00.09 --MUST INSTALL--	Critical	1	0	0	0	1	100%
Microsoft Data Access Components (MDAC) 2.7 SP1a (SEE NOTES)	Critical	1	0	0	0	1	100%
MS03-023 823559: Buffer Overrun In HTML Converter Could Allow Code Execution	Critical	0	1	0	0	1	100%
MS03-024 817606: Buffer Overrun in Windows Could Lead to Data Corruption	Critical	0	1	0	0	1	100%
MS03-025 822679: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation	Critical	0	1	0	0	1	100%
MS03-026 823980: Buffer Overrun In RPC Interface Could Allow Code Execution	Critical	0	1	0	0	1	100%
Microsoft .NET Framework 1.0 SP2	Critical - 01	0	1	0	0	1	100%
MS00-084 Q278499: Patch Available for 'Indexing Services Cross Site Scripting' Vulnerability	Critical - 01	1	0	0	0	1	100%
MS01-022 - Q296441: WebDAV Service Provider Can Allow Scripts to Levy Requests as User	Critical - 01	1	0	0	0	1	100%
MS01-033 - CODE RED-Q300972 Unchecked Buffer in Index Server ISAPI Extension	Critical - 01	1	0	0	0	1	100%
MS02-008 - XMLHTTP Control Can Allow Access to Local Files for MSXML 2.6	Critical - 01	0	1	0	0	1	100%

patchlink Deploy Export

- Vulnerability Analysis

This section displays the analysis results from the Discover Applicable Updates process on the computer. The analysis gives a simple top-down view of vulnerability patch status. The total number of vulnerabilities is displayed just above the table in the top right corner.

The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. [See Section 5; Vulnerabilities](#), [Section 6; Inventory](#), and [Section 7; Packages](#) for more detailed information.

10.11 Page Functions

- Information Tab

Selecting this tab will display additional Computer Information.

- Inventory Tab

Selecting this tab will display the Inventory for the computer.

- Deployments Tab
Selecting this tab will display the deployments that the computer has been assigned to.

10.12 Action Menu



- Deploy
This creates a deployment for the selected vulnerability. See [Section 9: Deploying Packages: Schedule Deployment Wizard](#) for more information.
- Export
Export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

10.13 Computer Vulnerability Security

*The Computer Vulnerabilities section of PLUS requires the **View Vulnerabilities Page** access right. If a user does not have the correct access the access denied error message is displayed.*

*To be able to change the filter from detected vulnerabilities to disabled or all requires the **Change Vulnerability Filter** access right. If a user does not have the correct access, the filter will not have any options to choose from.*

*To be able to view the associated distribution packages for a given vulnerability requires the **View Packages** access right. If a user does not have the correct access, the link on the package status image is disabled.*

*To be able to create a deployment based on the vulnerability analysis requires the **Deploy Vulnerabilities** access right. If a user does not have the correct access, the **Deploy** button is disabled.*

*To export all of the vulnerability analyses to a comma-separated value (CSV) file requires the **Export Vulnerability Data** access right. If a user does not have the correct access, the **Export** button is disabled.*

*To restart the discovery and analysis process for all of the computers registered to the PLUS requires the **Manage System Tasks** access right. If a user does not have the correct access, the **Scan Now** button is disabled.*

*To be able to view the computer inventory section requires the **View OS Inventories** access right. If a user does not have the correct access, the **Inventory** tab is disabled.*

*To be able to view the computer deployments section requires the **View Deployment Status** access right. If a user does not have the correct access, the **Deployments** tab is disabled.*

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

10.14 Computer Inventory Summary

The following inventories are gathered while in the discovery and analysis process: Operating Systems, Installed Software, Hardware and their device drivers, and Services. The Filter changes the display between the different inventories. When displaying the Inventory based on a single computer, the Operating Systems inventory is the initial inventory displayed.

The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. [See Section 5; Vulnerabilities](#), [Section 6; Inventory](#), and [Section 7; Packages](#) for more detailed information.

Computers PATCHLINK

Home | Reports | Inventory | Packages | **Computers** | Groups | Users | Options | Help | Server Time: 7/17/2003 3:02:02 PM (GMT-07:00)

Inventory Summary by Computer: \\BIG-MISTAKE Filter By: Software

Information | Reports | **Computer Inventory** | Deployments Total: 17

Software Programs	Count
Adobe Reader 6.0	1
BigFix Enterprise Client	1
BigFix Enterprise Console	1
BigFix Enterprise Server	1
BigFix Enterprise Suite Installation Generator (Evaluation)	1
HSP56 MR Drivers	1
Microsoft Internet Explorer 5.5 SP2	1
MSDE 2000 (BigFix Enterprise Database)	1
PatchLink Update Agent	1
SiS 900 PCI Fast Ethernet Adapter Driver	1
SiS Audio Driver	1
SiS630 730 V2.03	1
UpdateEXPERT 6	1
UpdateEXPERT UEAgent	1
Windows 2000 Hotfix (SP4) Q329553	1
Windows 2000 Hotfix (SP4) Q811114	1
Windows 2000 Hotfix (SP4) Q811493	1

patchlink Export Scan Now

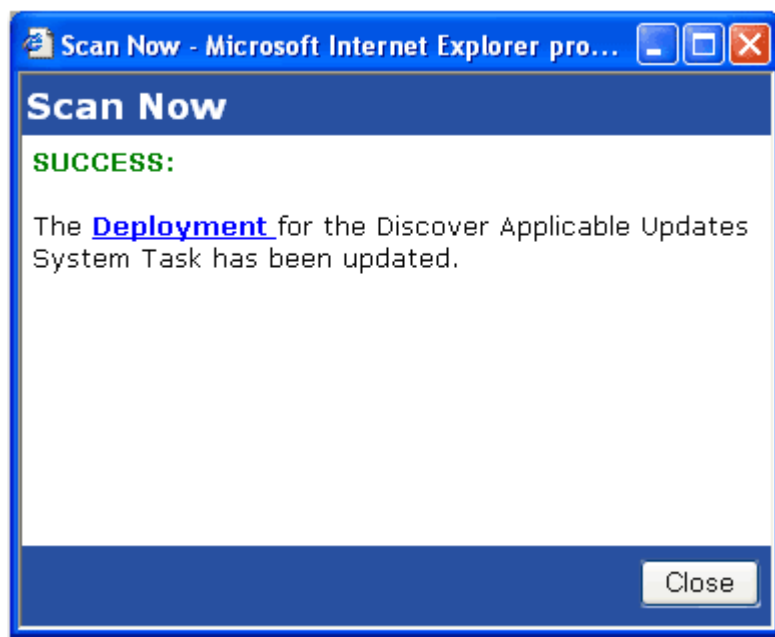
10.15 Page Functions

- **Information Tab**
Selecting this tab will display additional Computer Information.
- **Vulnerabilities Tab**
Selecting this tab will display the results of the Discovery and Analysis process for the Vulnerability.
- **Deployments Tab**
Selecting this tab will display the deployments that the computer has been assigned to.

10.16 Action Menu

- **Export**
Export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to all selected computers.

PLUS will reschedule the computer and initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.



Upon clicking the Close button on the screen, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

10.17 Computer Inventory Security

The Computer Inventory section of PLUS requires the [View OS Inventories](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the [Software](#) inventory requires the [View Software Inventories](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the [Hardware](#) inventory requires the [View Hardware Inventories](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the [Services](#) inventory requires the [View Services Inventories](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the [View Computers](#) access right. If a user does not have the correct access, the hyperlink on the inventory item is disabled.

To export the inventory to a comma-separated value (CSV) file requires the [Export Inventory Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

To be able to view the vulnerability results for the computer requires the [View Vulnerabilities](#) access right. If a user does not have the correct access, the [Vulnerabilities](#) tab is disabled.

To be able to view the computer deployments section requires the [View Deployment Status](#) access right. If a user does not have the correct access, the [Deployments](#) tab is disabled.

10.21 Computer Deployments Security

The computer deployments section requires the [View Deployment Status](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the vulnerability results for the computer requires the [View Vulnerabilities](#) access right. If a user does not have the correct access, the [Vulnerabilities](#) tab is disabled.

To be able to view the computer inventory section requires the [View OS Inventories](#) access right. If a user does not have the correct access, the [Inventory](#) tab is disabled.

To be able to view the computer deployments section requires the [View Deployment Status](#) access right. If a user does not have the correct access, the [Deployments](#) tab is disabled.

To be able to export the computer deployment data requires the [Export Deployment Data](#) access right. If a user does not have the correct access, the Export button is disabled.

Contact your PatchLink Administrator for more information on PatchLink Update Security.

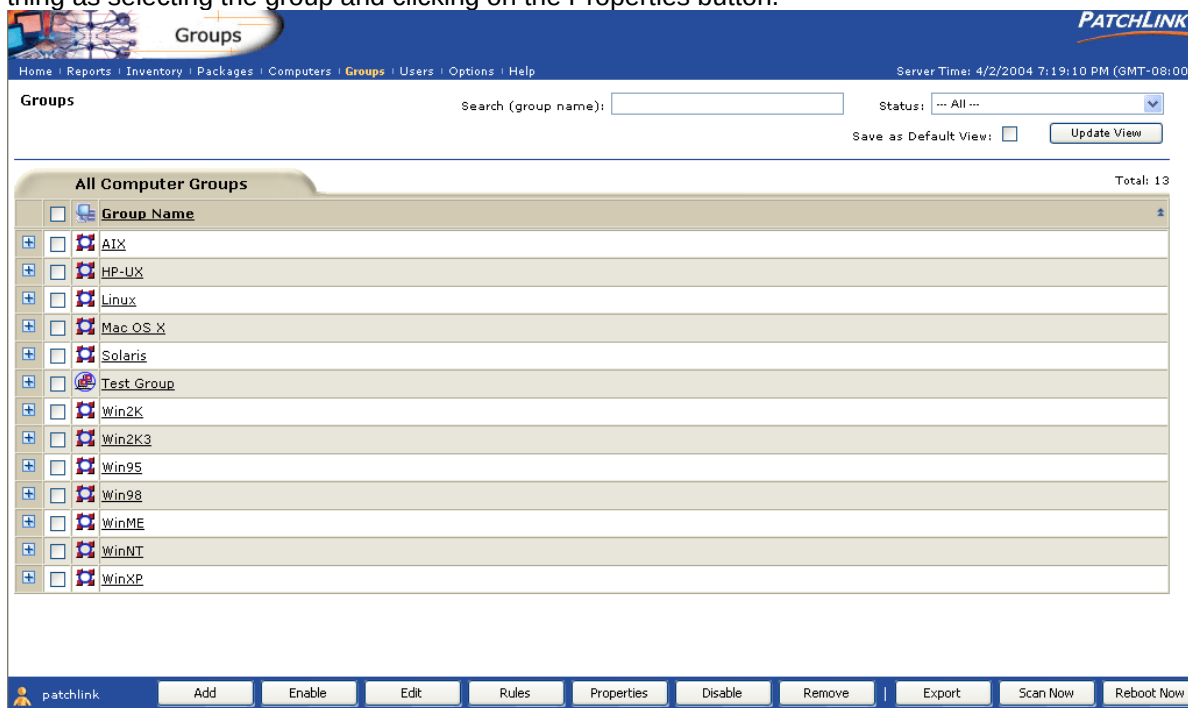
11. Groups

Home | Vulnerabilities | Inventory | Packages | Computers | **Groups** | Users | Reports | Options | Help

A group is a collection of computers for the purpose of making deployments on a “groupwise” basis.

The purpose is based upon user specification to provide an easier way to manage the entire group rather than managing each computer one at a time.

Clicking on the group name will display the group information and properties page. This is the same thing as selecting the group and clicking on the Properties button.



- With a group you can:
 - Deploy a distribution package (from an associated Vulnerability or local distribution package) to all computers of the group. When deploying from the Vulnerabilities section, the only computers which will receive the distribution package are the ones that are applicable to the vulnerability.
 - Define a set of policies which determine the behavior of the agents installed on those computers.
 - Define a baseline of Vulnerabilities or local distribution packages which are declared as mandatory. This ensures that these baseline items must be installed or detected as patched; else the deployments for those items will be auto-generated for immediate execution.
 - View the results of the Vulnerability Analysis for the entire membership of the group.

- View the results of the detected Inventory for the entire membership of the group.
- Reschedule the Discovery and Analysis process (Discover Applicable Updates System Task) to verify the Inventory and Vulnerabilities data is current.

11.1 Group Status

This displays the various groups that have been pre-generated by PLUS or user-defined by the local administrator. Each group entry displays the name of the group plus the status and type of the group.



Status	Description
	This is an enabled system group. One system group is formed automatically corresponding to each operating system in the network.
	This is a disabled system group. One system group is formed automatically corresponding to each operating system in the network. Vulnerabilities cannot be deployed to computers in this group.
	This is an enabled system group. These are the groups which are manually created by the administrator. Either one agent or multiple agents belonging to multiple operating systems can be added to a group.
	This is a disabled system group. These are the groups which are manually created by the administrator. Either one agent or multiple agents belonging to multiple operating systems can be added to a group. Vulnerabilities cannot be deployed to computers in this group.

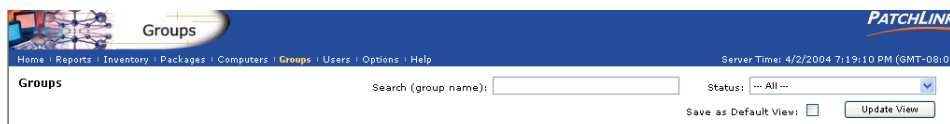
11.2 Page Functions

- Display and Hide

Click the to display additional information and statistics about the represented item. Click the to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (,) is only available for Microsoft Internet Explorer at this time.

- Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Groups page header.



- Search

Search (group name):

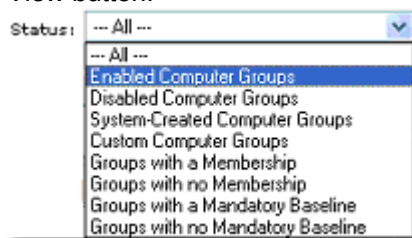
You may search Groups for more granular results by entering the group name text into the **Search** field and clicking on the  Update View button.

This will return the Group(s) having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

- Status

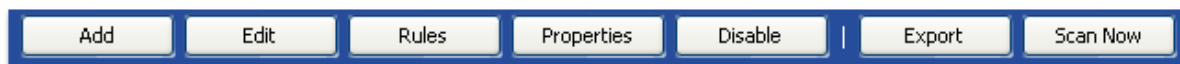
Filter by Status using the dropdown menu and click on the  Update View button.



This will return the Group(s) having the selected status. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

11.3 Action Menu



- Add

Clicking this button will bring up the Group Property page allowing new groups to be created [See Section 12; Add a Group Wizard](#) for more information.

- Edit

By clicking on the button, a edit group wizard comes up in which u can enter all the information about the already existing group. [See Section 12; Add a Group Wizard](#) for more information.

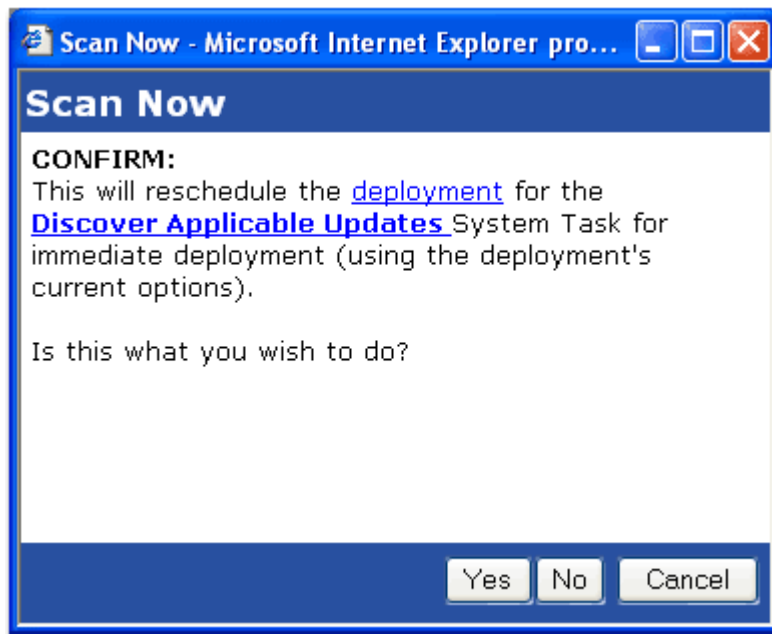
- Rules

Clicking the Rules button allows the PatchLink User the ability to create and populate a group based on a few minimal parameters. Group Name, Group Description, and a comma-delimited list of computer names (Windows computers must be prefixed with \\) may be entered.

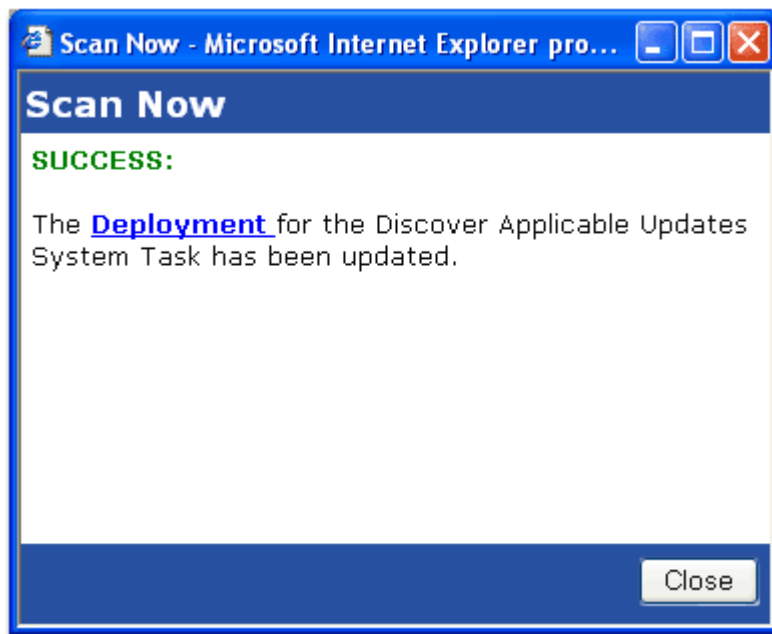
- **Properties**
Selecting a group and clicking on this button will display the group information and properties page.
- **Disable**
This disables all group-based functionality for the group members.
- **Enable**
This enabled all of the group-based functionality for the group members.
- **Remove**
This will delete all selected disabled groups.
- **Export**
Export the group data to a comma-separated value (CSV) file. The amount and order of the data is based on what the Group List view is filtered and sorted on.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected groups.

To initialize (choose) all groups, click on the Scan Now button without selecting any groups **or** select a group (or Groups) by clicking in the checkbox and click the **Scan Now** button.

If you choose to not select any groups, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the members for all of the groups.



To reschedule the **Discover Applicable Updates**, select Yes.



PLUS will reschedule the selected group(s)'s membership (or all groups' memberships), initialize a pop-up screen stating its success, and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Groups page will be refreshed and initialized. Previously selected deployment options are maintained.

11.4 Groups Security

The [Groups](#) section of PLUS requires the [View Groups](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to create, edit, enable, disable, and remove groups requires the [Manage Groups](#) access right. If a user does not have the correct access, the [Add](#), [Edit](#), [Rules](#), [Enable](#), [Disable](#) and [Remove](#) buttons are disabled.

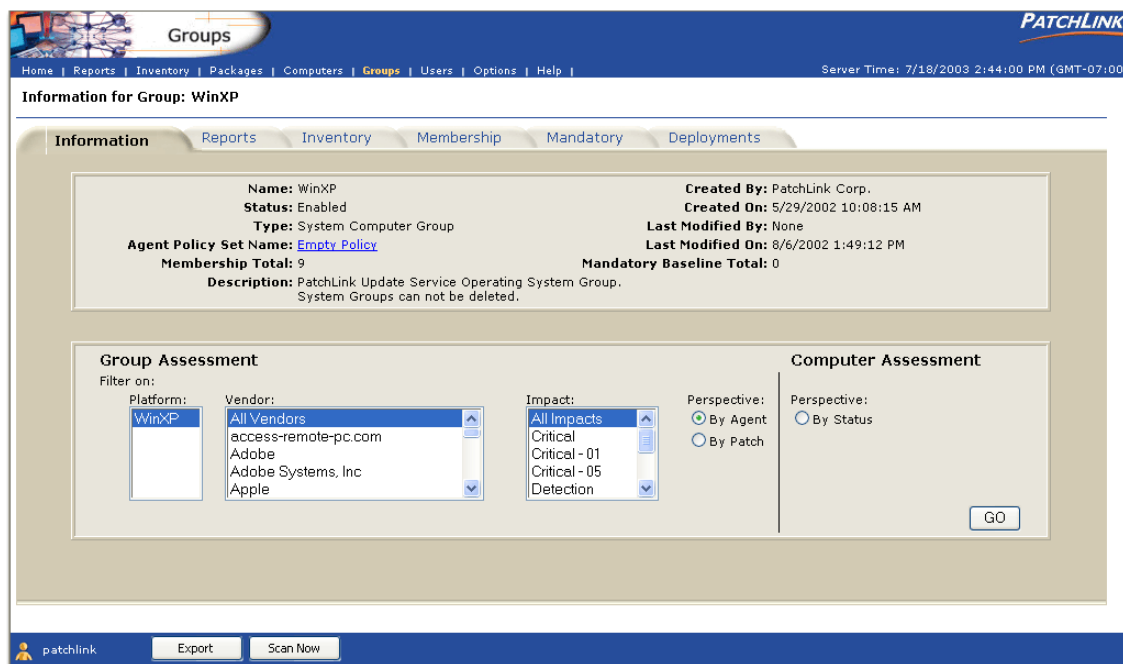
To export all of the group data to a comma-separated value (CSV) file requires the [Export Group Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

To reschedule the discovery and analysis process ([Discover Applicable Updates](#) System Task) for all members of the selected groups requires the [Manage System Tasks](#) access right. If a user does not have the correct access, the [Scan Now](#) button is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

11.5 Group Information

The group information and properties section of PLUS displays group related information, properties, and assessment graphs for viewing various statuses concerning the group's membership. Click on the actual group name link. The information tab of the Computer Information page (default) appears. (Win XP, All vendors, All Impacts, By Agent is used as an example)



- Information
 - Name: This displays the name of the group.

- Status: This displays the current status of the group.
 - Type: This displays the type of the group with respect to how it was created.
 - Agent Policy Set Name: This displays the assigned Agent Policy Set name and link to view the agent policy set information.
 - Membership Total: This displays the total number of computers which are a member of the group.
 - Created By: This displays the user who created the group.
 - Created On: This displays when the group was created.
 - Last Modified By: This displays the user who last modified the group.
 - Last Modified On: This displays when the group was last modified.
 - Mandatory Baseline Total: This displays the total number of patches which create the baseline for the group.
 - Description: This displays the group's description.
- Group Assessment

There are three basic graphs that can display status information about the group's membership. Selecting any one of the three options and clicking the **Go** button will initialize a graphical representation pie chart screen illustrating the assessment.

Group Patch Status by Agent

This displays the how many agents are in each of the following patch statuses:

- Fully Patches: the computer requires no additional patches at this time.
- Partially Patched: the computer is not fully patched, but has some patches are installed.
- Not Patched: The computer contains is not patched at all.
- Detecting: In process of running the Discovery and Analysis Process
- Pending: The initial Discovery and Analysis process has not started so there is no data on which to determine the status.

Additionally there are three filters that can define down to obtain more precise status information. The filters are:

- Platform
- Vendor
- Vulnerability Impact

Group Patch Status by Patch

This displays the how many applicable patches are in each of the following patch statuses:

- Fully Patches: the computer requires no additional patches at this time.
- Partially Patched: the computer is not fully patched, but has some patches are installed.
- Not Patched: The computer contains is not patched at all.
- Detecting: In process of running the Discovery and Analysis Process

- Non-applicable: The number of computers which have no Vulnerabilities applicable to them.
Additionally there are three filters that can define down to obtain more precise status information. The filters are:
 - Platform
 - Vendor
 - Vulnerability Impact

Agent Status

This displays the number of computers in each of the various agent states. The various states are:

- Sleeping: these computers are outside their defined hours of operation.
- Offline: these computers haven't contacted PLUS in over two communication intervals (15 minutes minimum for intervals smaller than 10 minutes).
- Running: these computers are currently running the Discovery and Analysis process and they do not correspond to a registered Deployment agent.
- Idle: these computers are active yet not performing any deployments.
- Working: these computers are working on some deployments.
- Disabled: these computers are disabled and will be given no work to do.

11.6 Lock Information

If a PatchLink User has locked a group's vulnerabilities, software, hardware or services, then information about the lock is displayed here.

- Lock Type

This displays what type of group lock was done. The four various types are:

- Group Vulnerability Locks
- Group Inventory Software Locks
- Group Inventory Hardware Locks
- Group Services Hardware Locks

- Total Locked

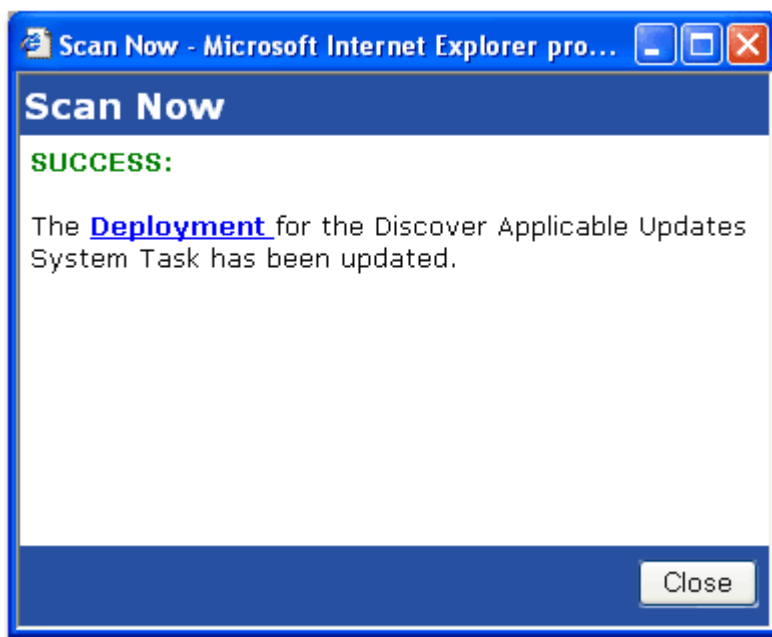
This displays the total number of items which were locked.

- Last Locked By: This displays who locked the group.
- Last Locked On: This displays when the group was locked.
- Lock Notes: This displays any notes that were added when the group was locked.

11.7 Action Menu



- **Export**
Export the group information to a comma-separated value (CSV) file.
- **Scan Now**
Initializes a screen that allows you to reschedule the deployment of the [Discover Applicable Updates](#) System Task for immediate execution to all enabled group members. Previously selected deployment options are maintained.



PLUS will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on screen, the Groups page will be refreshed and initialized. Previously selected deployment options are maintained.

11.8 Security

The Group Information and Properties section requires the [View Groups](#) access right. If a user does not have the correct access, the access denied error message is displayed.

To export all of the group information data to the comma-separated value (CSV) file requires the [Export Group Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

To restart the discovery and analysis process for all of the computers registered to the PLUS requires the [Manage System Tasks](#) access right. If a user does not have the correct access, the [Scan Now](#) button is disabled.

The Vulnerabilities tab requires the [View Vulnerabilities](#) access right. If a user does not have the correct access, the [Vulnerabilities](#) tab is disabled.

The Inventory tab requires the [View Software Inventory](#) access right. If a user does not have the correct access, the [Inventory](#) tab is disabled.

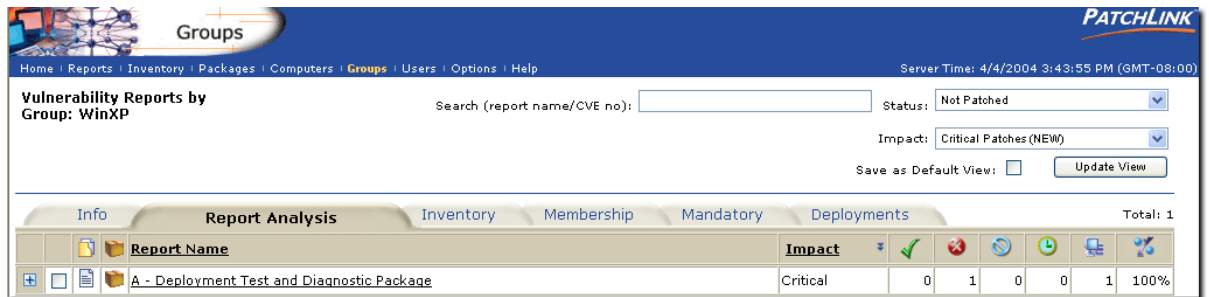
The Membership tab requires the [View Computers](#) access right. If a user does not have the correct access, the [Membership](#) tab is disabled.

The Deployments tab requires the [View Deployment Status](#) access right. If a user does not have the correct access, the [Deployments](#) tab is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

11.9 Vulnerabilities by Group

A Vulnerability consists of the vulnerability description, the signatures and fingerprints required to determine whether the vulnerability is patched or not patched, and the associated package or packages for performing the patch.



- Vulnerability Analysis**
 This section displays the analysis results from the Discover Applicable Updates process on each computer. The analysis gives a simple top-down view of vulnerability patch status. The various statuses are detailed below.

[See Section 5; Vulnerabilities](#), for more information.

11.10 Page Functions

- Display and Hide**
 Click the to display additional information and statistics about the represented item. Click the to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (,) is only available for Microsoft Internet Explorer at this time.
- Advanced Page Search, Filtering, and View Saving**
 The advanced page search, filtering dropdown menus, and saving functions appear in the Groups Vulnerability Analysis page header.

- Search**

Search (report name/CVE no):

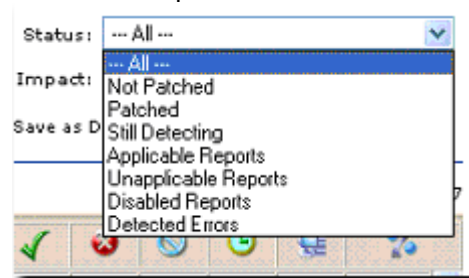
You may search vulnerabilities for more granular results by entering the vulnerability name (CVE; Common Vulnerabilities and Exposures) text into the **Search** field and clicking on the Update View button.

This will return the vulnerabilities having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

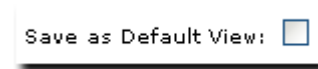
Save as Default View: ☐

- **Status**

Filter by Vulnerability Status using the dropdown menu and click on the  Update View button.



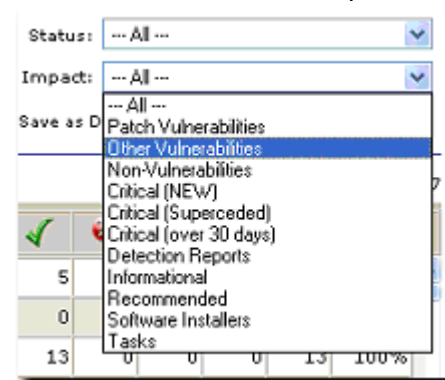
This will return the vulnerabilities having the selected status. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



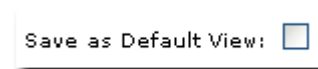
- **Impact**

Filter by Vulnerability impact levels using the dropdown menu and click on the  Update View button.

This is extremely useful when you want to find or display only the Vulnerabilities that, for example, are Critical (NEW).



This will return the vulnerabilities having the selected impact. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



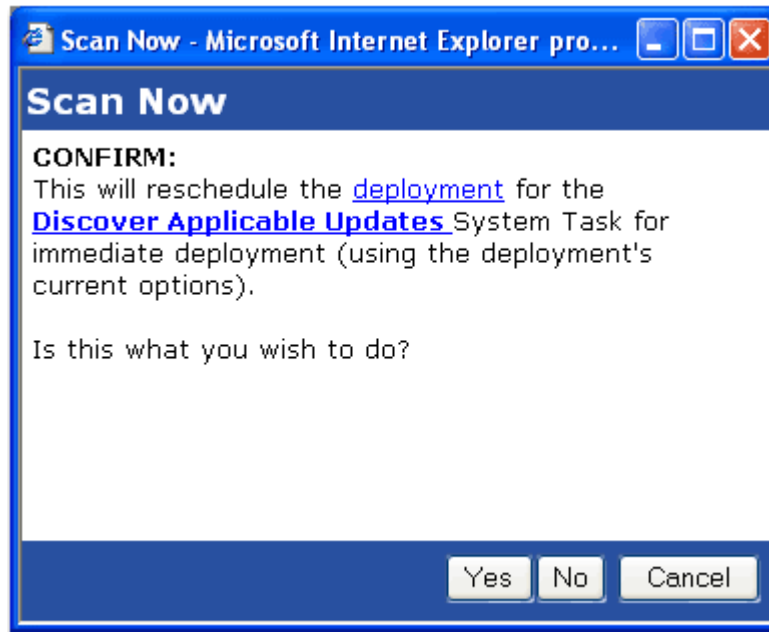
11.11 Action Menu



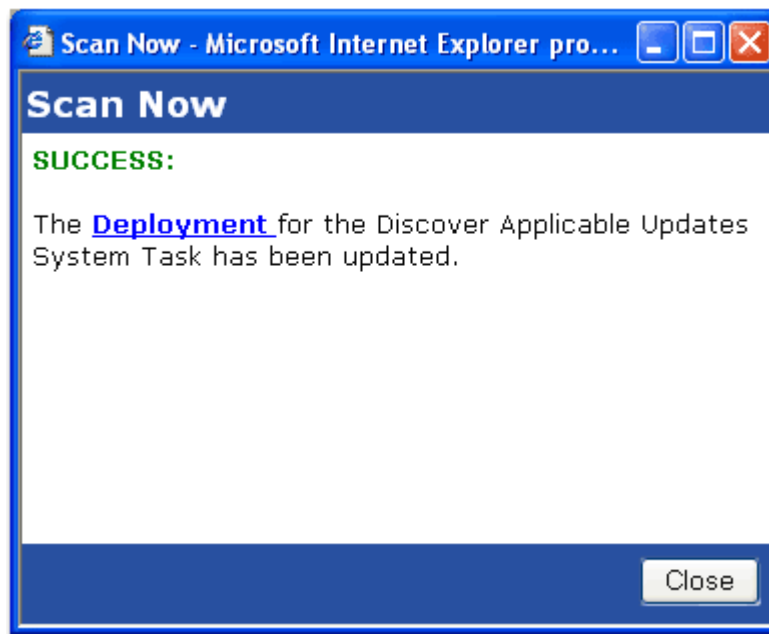
- **View**
To display additional information about the vulnerability for this group computer, select a vulnerability and click on the View button. This performs the same function as clicking on the name of the vulnerability.
- **Deploy**
Deploy the selected vulnerabilities associated update packages. See [Section 9: Deploying Packages: Schedule Deployment Wizard](#) for more information.
- **Lock**
Locks vulnerabilities for this group and its computer members.
- **Unlock**
Unlocks vulnerabilities for this group and its computer members
- **Enable**
To enable selected disabled computers, click on the Enable button.
- **Disable**
To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.
- **Export**
Export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.
- **Update Cache**
Deploys all of the **Discover Applicable Updates System Task** to all computers (or selected computers).
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to all selected groups.

To initialize (choose) all groups, click on the Scan Now button without selecting any groups and click the **Scan Now** button.

If you choose not to select any groups, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the groups.



To reschedule the **Discover Applicable Updates**, select Yes.



PLUS will reschedule the selected groups(s)'s membership (or all groups' memberships), initialize screen stating its success and provide a **Deployment** link to initialize a new screen with the results of the Discover Applicable Updates Deployment.

Upon clicking the **Close** button on the screen, the Groups page will be refreshed and initialized.

Previously selected deployment options are maintained.

11.12 Group Vulnerability Security

The Vulnerabilities section of PLUS requires the [View Vulnerabilities Page](#) access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the detailed vulnerability analysis requires the [View Vulnerability Details](#) access right. If a user does not have the correct access, the hyperlink will not be shown and the [View](#) button is disabled.

To be able to change the filter from detected vulnerabilities to disabled or all requires the [Change Vulnerability Filter](#) access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability requires the [View Packages](#) access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the vulnerability analysis requires the [Deploy Vulnerabilities](#) access right. If a user does not have the correct access, the [Deploy](#) button is disabled.

To be able to enable or disable vulnerabilities from being available by the discovery and analysis process requires the [Manage Vulnerabilities](#) access right. If a user does not have the correct access, the [Enable](#) and [Disable](#) buttons are disabled.

To be able to lock or unlock the results of the selected vulnerability analysis for the group's membership requires the [Manage Group Vulnerability Locks](#) access right. If a user does not have the correct access, the [Lock](#) and [Unlock](#) buttons are disabled.

To export all of the vulnerability analyses to a comma-separated value (CSV) file requires the [Export Vulnerability Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

To restart the discovery and analysis process for all of the computers registered to the PLUS requires the [Manage System Tasks](#) access right. If a user does not have the correct access, the [Scan Now](#) button is disabled.

To cache the associated distribution of the selected vulnerabilities requires the [Cache Packages](#) access right. If a user does not have the correct access, the [Update Cache](#) button is disabled.

The Inventory tab requires the [View Software Inventory](#) access right. If a user does not have the correct access, the [Inventory](#) tab is disabled.

The Membership tab requires the [View Computers](#) access right. If a user does not have the correct access, the [Membership](#) tab is disabled.

The Deployments tab requires the [View Deployment Status](#) access right. If a user does not have the correct access, the [Deployments](#) tab is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

11.13 Group Inventory Summary

This view will display the software, hardware, operating systems and services that were detected on the computers in the group. When displaying the Inventory based on a single computer, the Software inventory is the initial inventory displayed.

This view is the same as the Inventory Summary view with the following differences:

1. Only displays the inventory based upon the member computers of the selected group.
2. The Scan Now button will only reschedule the **Discover Applicable Updates System Task** for the selected group's membership.

See [Section 6: Inventory](#) for more detailed information.

Information	Reports	Group Inventory	Membership	Mandatory	Deployments	Total: 24
Software Programs						
Adobe Download Manager (Remove Only)						1
Adobe Reader 6.0						1
Command AntiVirus for Windows Enterprise						1
Internet Explorer Q818529						1
Java 2 Runtime Environment Standard Edition v1.3						1
Microsoft .NET Framework (English) v1.0.3705						1
Microsoft Internet Explorer 5.5 SP2						1
MSN Messenger 5.0						1
PatchLink Agent Deployment						1

- **Software Programs**
This displays the name of the software application.
- **Lock Status**
If the software is locked for the group this image indicates if the software application is in compliance or not.
- **Number of Instances**
The number of times this software application was detected.

11.14 Page Functions

- **Display and Hide**
Click the to display additional information and statistics about the represented item. Click the to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (,) is only available for Microsoft Internet Explorer at this time.

- Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Group Inventory page header.

- Search

Search (inventory name):

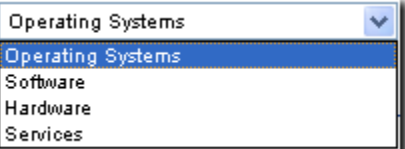
You may search inventory for more granular results by entering the inventory name text into the **Search** field and clicking on the  Update View button.

This will return the inventory having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

- Type

Filter by Type using the pull down menu and click on the  Update View button.

Type: 

This allows you to search for Operating Systems, Software, Hardware and Services.

- Operating Systems View

Displays the full operating system platform names and the number of instances, or times this operating system was detected.

- Software View

Displays the installed software applications and the number of instances, or times this software application was detected.

Software Programs

This displays the name of the software application. Click the  for a software application to display the list of computers for that application. Click on the  to close this list.

Number of Instances

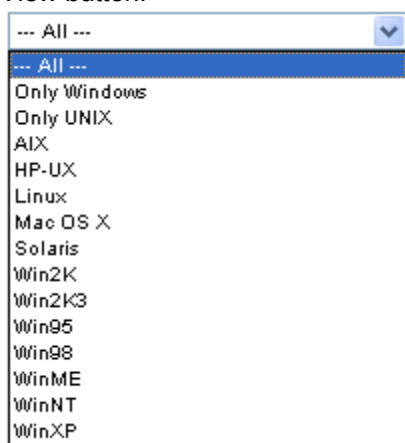
The number of times this software application was detected.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

- Groups

Filter by Group using the pull down menu and click on the  Update View button.



This allows the user to search on any user defined or server defined groups that exist.

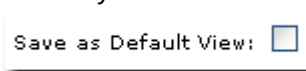
- o Operating Systems

Displays the selected or filtered operating system.

- o Number of Instances

This displays the number of times this operating system platform has been detected. For displaying the Operating System Inventory for a single computer, this is always one.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- Hardware View

Displays the client Hardware devices.

- o Hardware Device Class

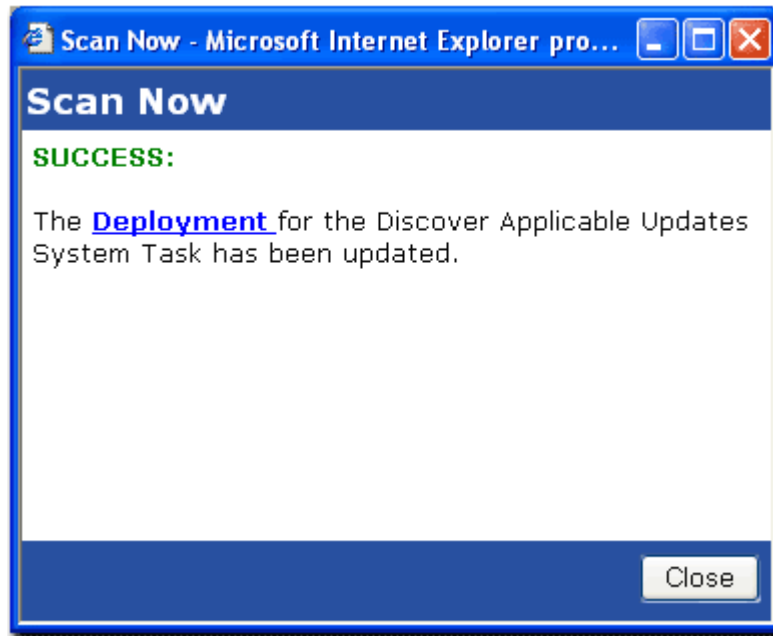
Hardware is separated into device classes such as disk drives, processors, network adapters, etc. Click the  to display the list of devices for each class, or click on the  to display them all (for a long list of devices this may take a few moments to generate). Click the  to close this list.

- o Device
A device is a specific piece of hardware, such as a “Microsoft USB IntelliMouse Optical”. Click the  for a device to display the list of computers for that device. Click the  to close this list.
- o Number of Instances
An Instance is a specifically detected device or installed driver. A computer may contain multiple instances of a installed device or driver. For example, a computer may contain a video graphics adapter that contains multiple video sources and destinations in which each source or destination is discovered as multiple instances of the same device or driver.
- Services View
Displays the detected services that may or may not be running.
 - o Service Name
This displays the name of the service.
 - o Number of Instances
The number of times this service was detected.

11.15 Action Menu



- Lock
Clicking on the lock button will lock the selected inventory for all computers members of the group. When the inventory changes for one of the computer members the inventory item is highlighted as being out of compliance and an e-mail notification is sent to the group notification list of the occurrence.
- Unlock
Clicking on the unlock button will clear the lock.
- Export
Clicking on the Information tab will display the Group Information and Properties page.
- Scan Now
Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to the selected groups.



PLUS will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a screen with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Groups page will be refreshed. Previously selected deployment options are maintained.

11.16 Group Inventory Security

The Group [Inventory](#) section of PLUS requires the [View Software Inventory](#) access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the [Operating Systems Inventory](#) requires the [View Inventory OS](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the [Hardware Inventory](#) requires the [View Hardware Inventory](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the [Services Inventory](#) requires the [View Services Inventory](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the [View Computers](#) access right. If a user does not have the correct access, the hyperlink and ,  more information images are disabled.

To export the inventory to a comma-separated value (CSV) file requires the [Export Inventory Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

The Vulnerabilities tab requires the [View Vulnerabilities](#) access right. If a user does not have the correct access, the [Vulnerabilities](#) tab is disabled.

The Membership tab requires the [View Computers](#) access right. If a user does not have the correct access, the [Membership](#) tab is disabled.

The Deployments tab requires the [View Deployment Status](#) access right. If a user does not have the correct access, the [Deployments](#) tab is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

11.17 Group Membership

The Group Membership section of PLUS displays all computers which are members of the group. Clicking on a computer name will allow you to display a computer's specific information.

This view is almost identical to the computers section of PLUS. See [Section 10; Computers](#) for more information.



- Computer Name**
 This displays the name of the computer. Click on the computer name to display specific information about the computer.
- Status**
 This displays the status of the computer.
- Platform**
 This displays the operating system platform the computer is running.
- OS Info**
 This displays additional information about the operating system the computer is running.
- Version**
 This displays the version of the agent running on the computer.
- Group List**
 This displays the list of groups that the computer is a member of.

11.18 Agent Status

Status	Description
	This is an idle deployment agent.
	This deployment agent is idle and has deployments in its work queue.
	The agent is sleeping as it is outside its hours of operation.
	The agent is sleeping as it is outside its hours of operation and has deployments in its work queue.
	This agent is currently working on a deployment.
	This is an enabled detection agent that does not correspond to a registered deployment agent ² .
	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes).
	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes) and has deployments in its work
	This agent has been disabled.

Additional information about the status of the agent is displayed once your mouse hovers over the image.

11.19 Page Functions

- Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Computers page header.

- Search

Search (computer name):

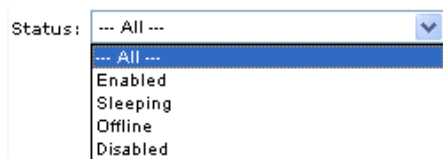
You may search computers for more granular results by entering the computer name text into the **Search** field and clicking on the  Update View button.

This will return the computer having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: ☐

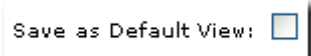
- **Status**

Filter by status using the dropdown menu and click on the  Update View button.



This allows the user to search on enabled, sleeping, offline, and disabled systems that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



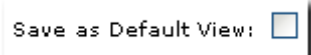
- **Groups**

Filter by group using the dropdown menu and click on the  Update View button.



This allows the user to search on any user defined or server defined groups that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



11.20 Action Menu



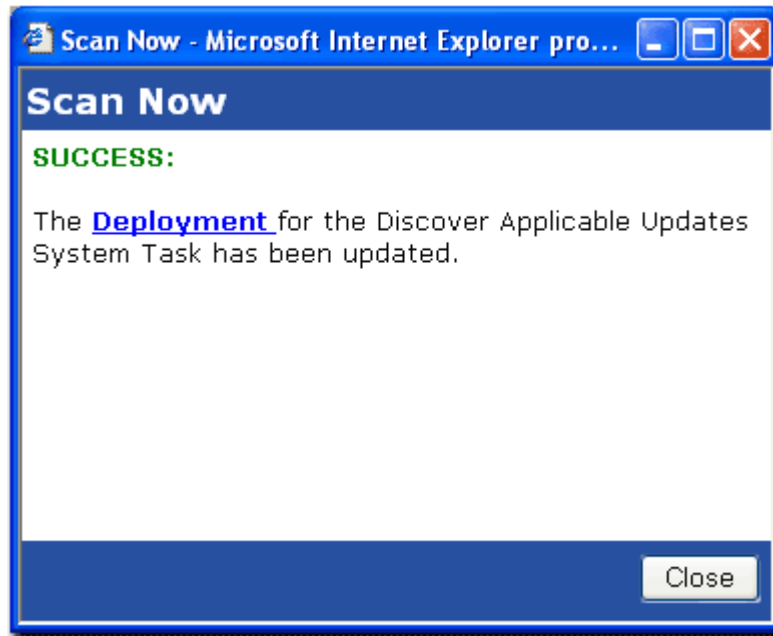
- **Install**
Click on the Install button to display the list of agent installers that can be used to register computers to PLUS.

The agent installer screen contains links to all of the agent installations and additional information on Operating Systems, Requirements, and Installation Notes.

See Item 11.4.; Install, for more information.
- **Manage**
Manage the group's computer membership. Initializes the Group Property page.
[See Section 12; Add a Group Wizard](#) for more information.
- **View**
To display additional information about the computer, select a computer and click on the View button. This performs the same function as clicking on the name of the computer.
- **Enable**
To enable selected disabled computers, click on the Enable button.
- **Deploy**
To deploy a package to specified computers within the computer membership, simply click the Deploy button, select the package, the computers, and the deployment options.

See [Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information.
- **Disable**
To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.
- **Export**
Exports the group membership information to a comma-separated value (CSV) file.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to the selected group.

PLUS will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a screen with the results of the Discover Applicable Updates Deployment.



Upon clicking the Close button on the screen, the Groups page will be refreshed. Previously selected deployment options are maintained.

11.21 Group Membership Security

The Group [Membership](#) section of PLUS requires the [View Group Membership](#) access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the Enabled [Group Membership](#) requires the [View Enabled Group Membership](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the [Disabled Group Membership](#) requires the [View Disabled Group Membership](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the [All Group Membership](#) requires the [View All Group Membership](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to utilize the [Scan Now](#) capability requires the [Scan Now](#) access right.

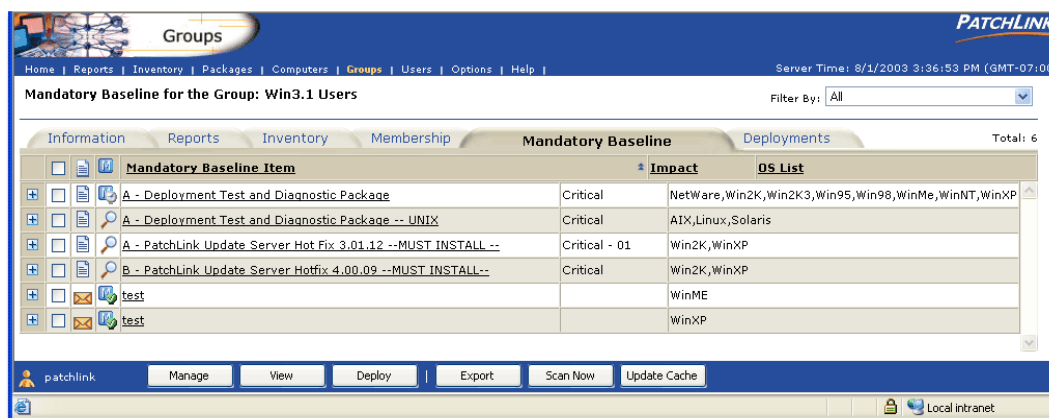
To be able to install, manage, view, deploy or disable group memberships requires the [Manage Group Membership](#) access right. If a user does not have the correct access, the [Install](#), [Manage](#), [View](#), [Deploy](#) and [Disable](#) buttons are disabled.

To export the inventory to a comma-separated value (CSV) file requires the [Export Group Membership Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

11.22 Groups Mandatory Baseline

Mandatory Baselines are the mandatory packages (defined by the user) for a computer group that will be delivered to all members.



Notes:

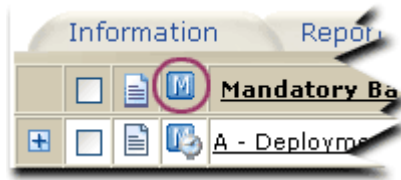
- Any non-system vulnerability with one or more associated packages can be associated with a given computer group as a Mandatory patch.
- Mandatory vulnerability-based patches shall be applied to every computer in the computer group which is of a compatible operating system type to the vulnerability.
- Mandatory vulnerability-based patches shall be applied to a given computer only when the vulnerability for that given computer shows a failure condition showing that the patch is not already installed on the computer.

The Group Summary shows three views of currently existing groups on the PatchLink Update Server. Select the desired **Filter by:** item from the upper right drop down menu to view the results. The views are:

- Vulnerabilities:** Show only the vulnerabilities
- Distribution Packages:** Show only the distribution packages
- All vulnerabilities:** Show all the mandatory baseline of the Groups that exist on the PatchLink Update Server.

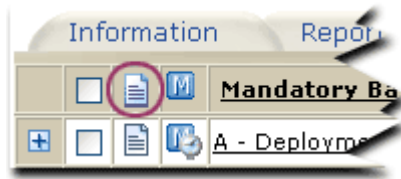
11.23 Status

There are two status columns for the Mandatory Baseline page. The first will display one of the following icons giving information about the patch itself:



Status	Description
	This is a current vulnerability.
	This is a new vulnerability.
	This is a disabled vulnerability.
	This is a distribution package.

The second column will display information about the group with respect to the patch using one of the following icons:



Status	Description
	At least one member of this group is either Detecting, Obtaining the Package, Waiting On Detection, or in a Deployment Not Started state. (None of the members have errors).
	At least one member of this group is Deploying this patch. (None of the members have errors, nor are they Detecting).
	All of the members of this group are Disabled for this patch.
	All of the members of this group are either Not Applicable or In Compliance for this patch. (Some can also be disabled).
	At least one member of this group is out of compliance. This indicates that an error has occurred. More specific information about the type of error will appear in the mouse over text.

- Mandatory Baseline Item:
Name of the item
- Impact:
If applicable, the impact of the Vulnerability
- OS List:
List of applicable Operating Systems

11.24 Select

To select a Mandatory Baseline you can:

- Click anywhere within the mandatory baseline entry line (be careful: *mandatory baseline item names* are links to view other information (see below).
- Click the checkbox for that mandatory baseline item and click the **View** button.
- Click the checkbox in the header section to select all of the mandatory baseline items.

Not Patched		Patched	Error	Detecting	Total Computers:1	
☐	Computer Name	☐	Other Name	Operating System	OS Version	Analysis Date
☐	\\SUPPORT-W2K	☐	support-w2k	Win2K	Win2K-Service Pack 3	8/1/2003 10:23:11 PM

This view is similar to the Vulnerabilities Section. See [Item 5.7 Vulnerability Analysis Details](#) for more details

At the View Mandatory deployment stage, you can select computers and schedule a deployment to them. Also, at this stage you get the complete statistics for the computers whose Detection Agents have run the detected vulnerability.

These computers are divided in 9 categories:

- Compliance
- Detecting
- Disabled
- Deploying
- Not Applicable
- Obtaining Package
- Deployment Not Started
- Waiting On Detection
- Error: {specific error message}

These are two error categories:

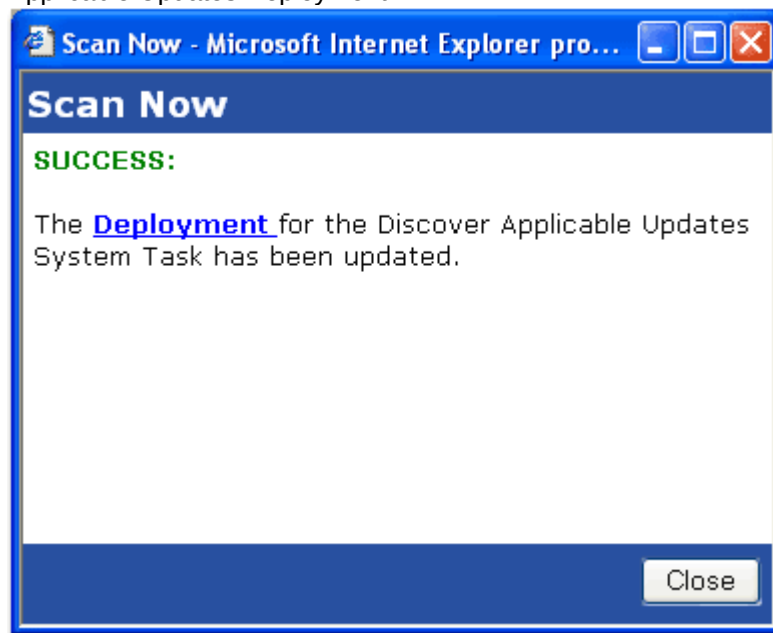
- Detection Errors
- Deployment Errors
- Item Type

11.25 Action Menu



- **Manage**
Initializes the Group Property Page to manage the baseline of the Group. [.See Section 12; Add a Group Wizard](#) for more information.
- **View**
Views the Vulnerability analysis for the Group.
- **Deploy**
Deploys the selected package to the specified Computer. See [Section 9; Deploying Packages: Schedule Deployment Wizard](#) for more information.
- **Export**
Exports the group mandatory baseline information to a comma-separated value (CSV) file.
- **Scan Now**
Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to the selected computer.

PLUS will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a screen with the results of the Discover Applicable Updates Deployment.



Upon clicking the Close button on the screen, the Groups page will be refreshed and initialized. Previously selected deployment options are maintained.

- Update Cache

Initiates the process to cache (or re-cache) for the selected distribution packages. If no distribution packages are selected this will re-cache all of the previously cached distribution packages.

11.26 Group Mandatory Baseline Security

The [Group Membership](#) section of PLUS requires the [View Group Mandatory](#) access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the [Group Mandatory Baseline](#) requires the [View Enabled Group Membership](#) access right. If a user does not have the correct access, the filter will not have this option available.

To be able to manage, view, deploy or disable group memberships requires the [Manage Group Membership](#) access right. If a user does not have the correct access, the [Manage](#), [View](#), [Deploy](#) and [Disable](#) buttons are disabled.

To be able to utilize the [Scan Now](#) capability requires the [Scan Now](#) access right

To cache the associated distribution of the selected vulnerabilities requires the [Cache Packages](#) access right. If a user does not have the correct access, the [Update Cache](#) button is disabled.

To export the inventory to a comma-separated value (CSV) file requires the [Export Group Membership Data](#) access right. If a user does not have the correct access, the [Export](#) button is disabled.

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

11.27 Group Deployments

This view displays the deployments that the selected group has been assigned to.

Note:

This view does not display the individual deployments each member has been assigned to, only the deployments that the group, as an entity, have been assigned to.

This view is the same as the Deployment Summary view, but displays all deployments that the selected group has been assigned to.

The screenshot shows the PATCHLINK web interface. The top navigation bar includes links for Home, Reports, Inventory, Packages, Computers, Groups, Users, Options, and Help. The server time is 8/4/2003 3:48:39 PM (GMT-07:00). The main content area is titled 'Deployments to Group: Win3.1 Users'. Below this, there are tabs for Information, Reports, Inventory, Membership, and Mandatory. The 'Group Deployments' tab is active, showing a table with columns: Name, Initial Start Date, and a series of status columns (1, 0, 1, 1, 1, 100%). The table lists four deployments:

Name	Initial Start Date	1	0	1	1	1	100%
Deployment of PatchLink Server HotFix TEST 4.00.9	8/1/2003 10:36:54 PM (UTC)	1	0	1	1	1	100%
Deployment of Deployment Test and Diagnostic Package	8/1/2003 10:35:26 PM (UTC)	1	0	1	1	1	100%
Deployment of test	8/1/2003 10:32:36 PM (UTC)	0	0	1	0	0	0%
Deployment of test	8/1/2003 10:32:36 PM (UTC)	0	0	1	0	0	0%

At the bottom of the table, there is a status bar with buttons: Abort, Enable, Change, Remove, Disable, and Export.

11.28 Action Menu



- **Abort**
Allows the user to abort the deployment for the group.
- **Enable**
Allows the user to enable the selected disabled deployments.
- **Change**
Allows the user to change the selected deployment.
- **Remove**
Allows the user to change the selected disabled deployment(s).
- **Disable**
Allows the user to disable the selected deployments.
- **Export**
Exports the group deployment(s) information to a comma-separated value (CSV) file.

11.29 Group Deployments Security

To be able to change, disable, enable, abort or remove a deployment(s) requires the **Manage Deployments** access right. If a user does not have the correct access, the **Change**, **Disable**, **Enable**, **Abort** and **Remove** buttons are disabled.

To export the inventory to a comma-separated value (CSV) file requires the **Export Group Membership Data** access right. If a user does not have the correct access, the **Export** button is disabled.

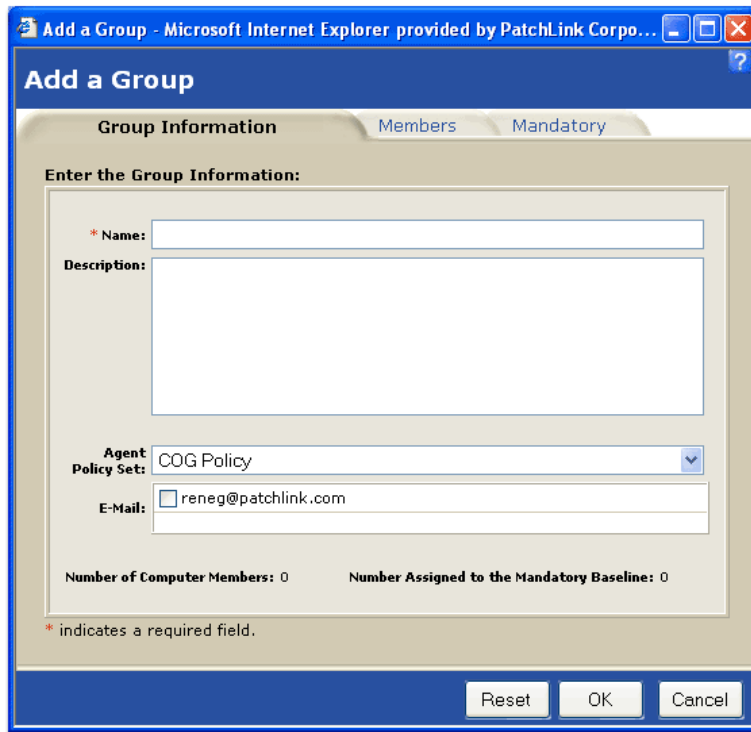
Contact your PatchLink Administrator for more information on PatchLink Update Security

12. Add a Group Wizard

Plus has the ability to add groups. From the **Groups** homepage, click on the **Add** button on the Action Menu.

12.1 Group Property Screen - Info

The **Group Information** Screen section of PLUS allows the PatchLink User the ability to create a group. System-defined groups cannot be changed. The **Group Information** tab of the property page contains the base information and it is this tab in which a group's information is loaded and saved.



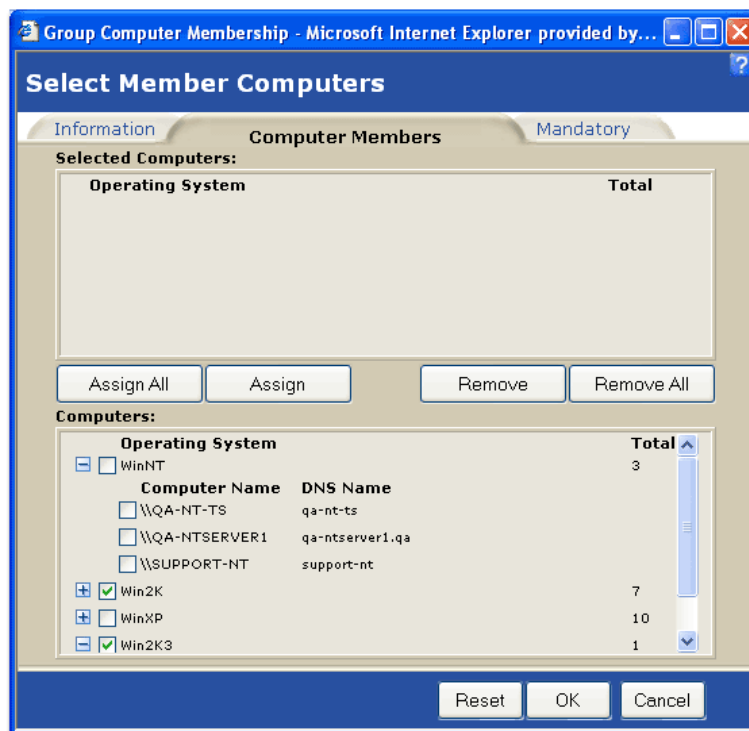
- **Group Name**
The name of the group to be created. This field is required for groups to be created.
- **Description**
Notes or information describing the group.
- **Agent Policy Set**
The desired Agent Policy Set to use for the computers who are members of the group. When a computer's policies are calculated, PLUS determines the superset of all Agent Policy Sets for the groups the computer is a member of. Thus, if one policy set says the agent has a 60 minute interval and another says the computer has a 30 minute interval, the resulting policy set is 30 minutes.

Set the Agent Policy Set to the Empty Policy if this group is to have to effect on the policy calculations.

- E-Mail
Select any users who have been added to the E-Mail Notification list on PLUS The selected users will be sent group-based notifications.
 - Number of Computer Members
The total number of computers that are in the selected group.
 - Number of Computers assigned to the Mandatory Baseline
The total number of computers who are currently assigned to the group.
- Screen Functions
 - Reset
Resets the page back to its initial state.
 - OK
Initiates the process to save the group. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
 - Cancel
Cancels the add process and closes the group property page window.

12.2 Group Property Screen - Members

The Computer Members Group Property Page section of PLUS allows the PatchLink User the ability to create a group. System-defined groups cannot be changed. The **Computer Members** tab of the property page contains a list of all computers which have been assigned as members of the group and the list of computers which are not a member of the group.



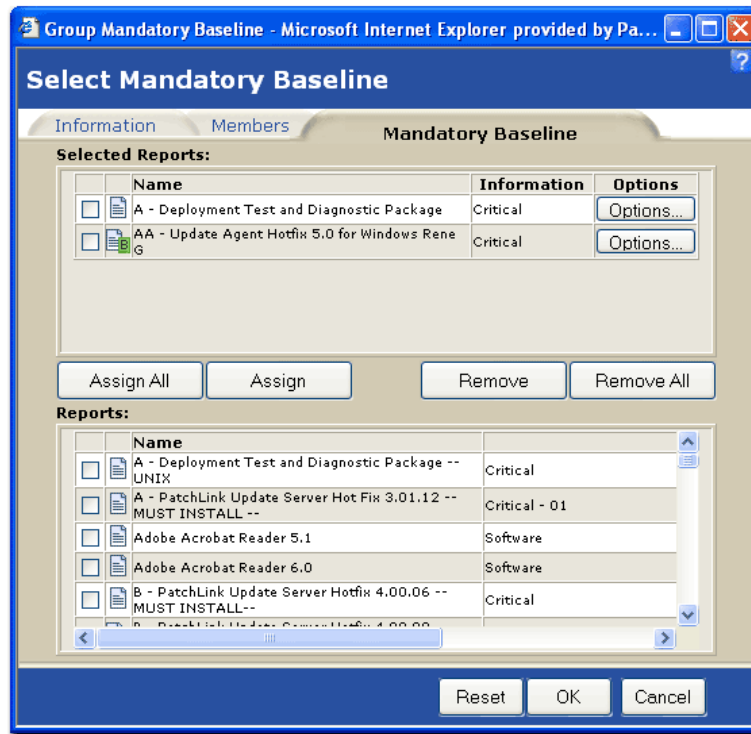
- Selected Computers
 - Operating System
The operating system platform name. Click the  to display the list of computers for that operating system. Click  to close the list.
 - Computer Name
The name of the computer.
 - DNS Name
The DNS name assigned to the computer
 - Total Selected per OS
The total number of computers that have been selected for the operating system platform.

- Available Computers
 - Operating System
The operating system platform name. Click the  to display the list of computers for that operating system. Click  to close the list.
 - Computer Name
The name of the computer.
 - DNS Name
The DNS name assigned to the computer
 - Total Selected per OS
The total number of computers that have not been selected for the operating system platform.

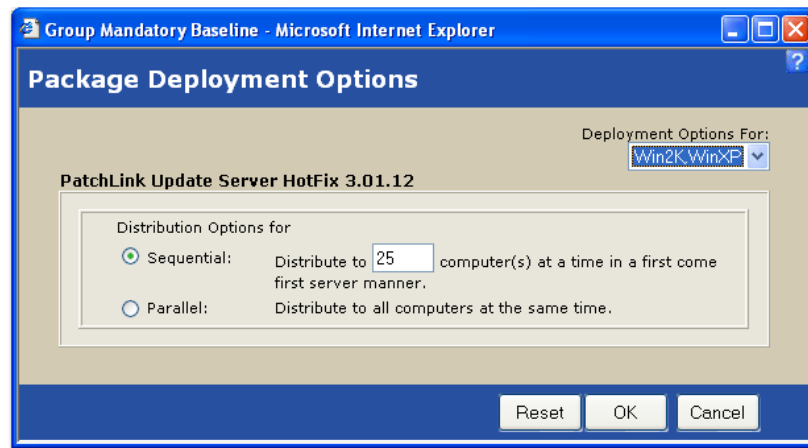
- Screen Functions
 - Assign All
Assigns all available computers to the group.
 - Assign
Assigns all available computers to the group.
 - Remove
Removes the selected computers from the group.
 - Remove All
Removes all selected computers from the group.
 - Cancel
Cancels the add process and closes the group property page window.
 - Reset
Resets the page back to its initial state.
 - OK
Initiates the process to save the group (or the group's changes). If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
 - Cancel
Cancels the add process and closes the group property page window.

12.3 Group Property Screen –Mandatory Baseline

The Group Property Page section of PLUS allows the **PatchLink User** the ability to create a group, system-defined groups cannot be changed. The **Mandatory Baseline** tab of the property page contains the lists of selected and available Vulnerabilities and Locally-created Distribution Packages for the group's baseline.



- Selected Baseline Items
 - Baseline Item Name
The name of the vulnerability or package.
 - Baseline Item Type
This is either a Vulnerability or a Distribution Package.
 - Information
This contains information about the operating systems for the package or the impact for a vulnerability.
 - Options
Click the Options button to display a screen with the deployment options and information about the item.

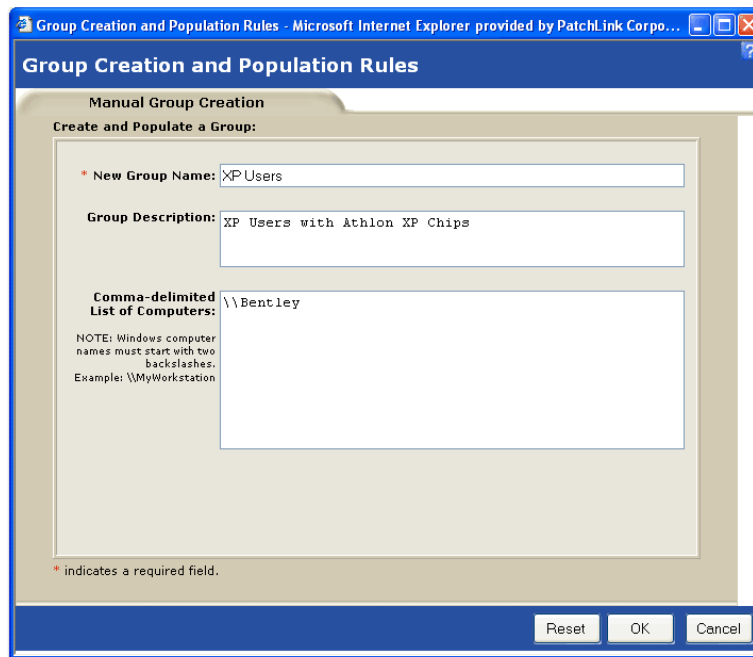


Sequential (default) indicates that only N (defaulted to 25) number of computers may perform this deployment at any given moment. The other computers will get the deployment, but it is on a first come first serve basis.

Parallel, or all computers may receive the deployment as they connect up to PLUS to get their tasks.

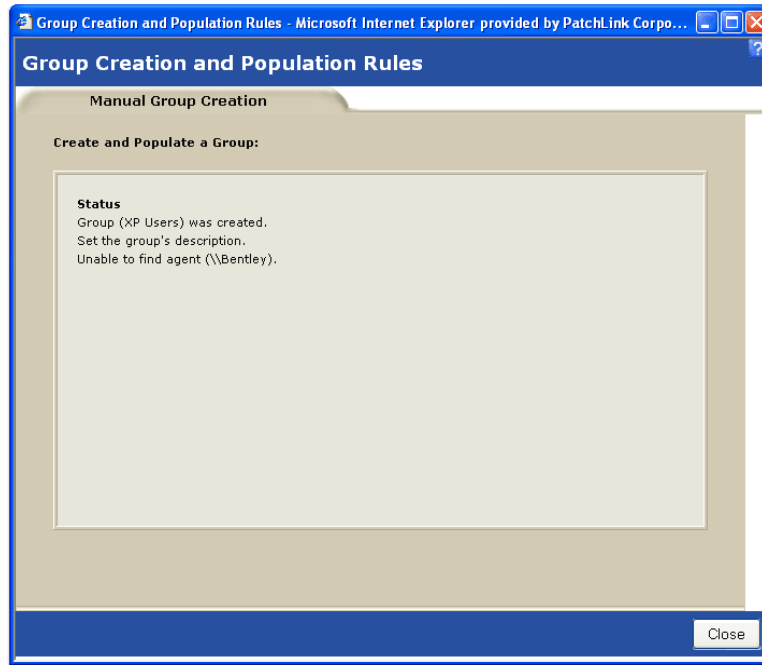
- Available Computers
 - Baseline Item Name
The name of the vulnerability or package.
 - Baseline Item Type
This is either a Vulnerability or a Distribution Package.
 - Information
This contains information about the operating systems for the package or the impact for a vulnerability.
- Screen Functions
 - Assign All
Assigns all available vulnerabilities and packages to the group.
 - Assign
Assigns all available vulnerabilities and packages to the group.
 - Remove
Removes the selected vulnerabilities and packages from the group.
 - Remove All
Removes all selected vulnerabilities and packages from the group.
 - Reset
Resets the page back to its initial state.

- **OK**
Initiates the process to save the group (or the group's changes). If a Mandatory Baseline item has been added which requires a license to agree prior to the saving of the group, a license agreement page will be displayed. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
 - **Cancel**
Cancels the add process and closes the group property page window.
 - **Options**
Displays a window with the deployment options for the item.
- **Edit**
Selecting a group and clicking on this button will bring up the Group Property screen with this group's information allowing the group to be changed. See [Section 13; Edit a Group Wizard](#) for more information.
 - **Rules**
Clicking this button will bring up the Manual Group Creation and Population Rules property page.



Define a new group by filling in a new group's name and description. The group will be auto-populated by adding in a comma-separated list of computer names.

Clicking the OK button initializes the Manual Group Creation status screen.



Upon clicking the Close button of the Manual Group Creation status screen, the **Groups Homepage** is automatically refreshed showing the newly created computer group.

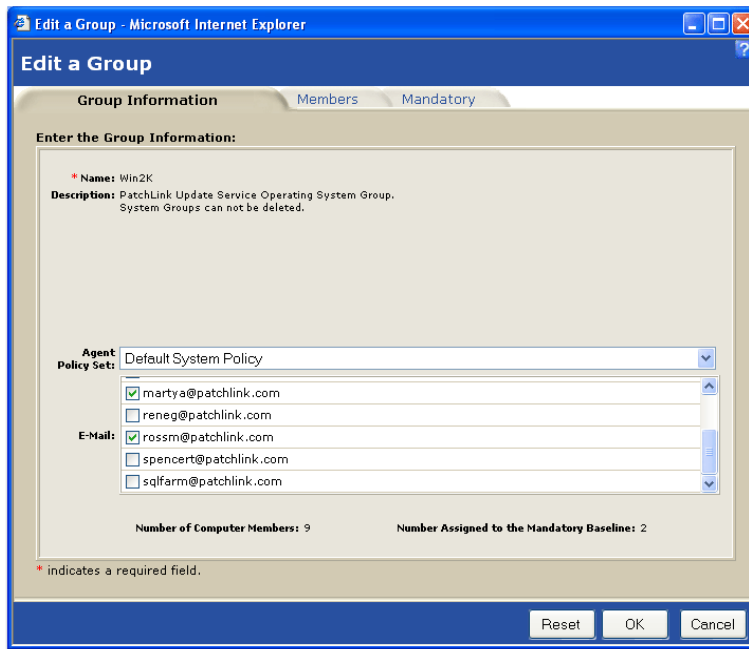
13. Edit a Group Wizard

Plus has the ability to edit groups. To Edit a group, you must first create one. [See Section 12: Add a Group Wizard](#) for more information.

From the **Groups** homepage, select the group that you wish to edit by clicking in the checkbox next to the item and click on the **Edit** button on the Action Menu.

13.1 Group Property Screen - Info

The **Group Information** Screen section of PLUS allows the PatchLink User the ability to edit a group. System-defined groups cannot be changed. The first tab of the property page contains the base information and it is this tab in which a group's information is loaded and saved.



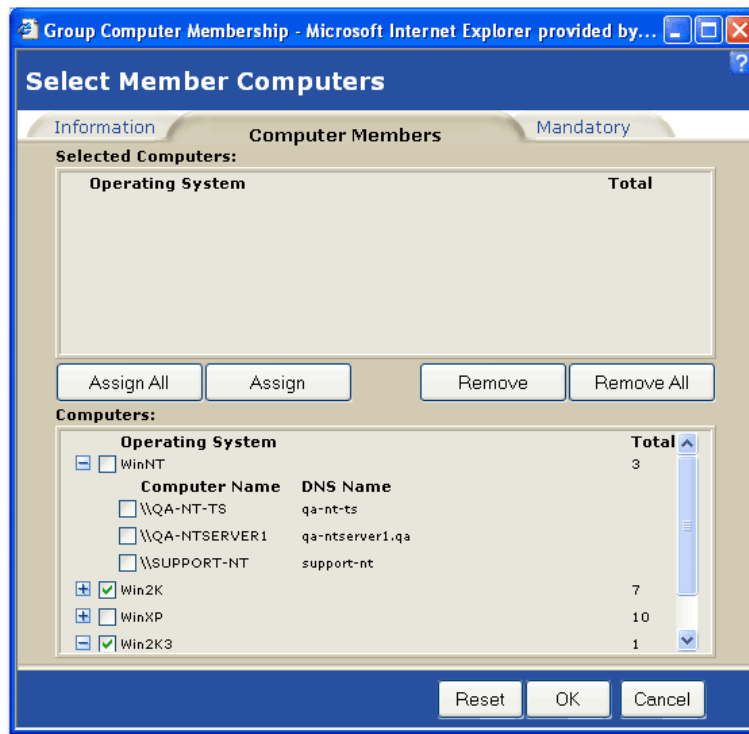
- **Group Name**
The name of the group selected to be edited.
- **Description**
Previously entered notes or information describing the group.
- **Agent Policy Set**
The desired Agent Policy Set to use for the computers who are members of the group. When a computer's policies are calculated, PLUS determines the superset of all Agent Policy Sets for the groups the computer is a member of. Thus, if one policy set says the agent has a 60 minute interval and another says the computer has a 30 minute interval, the resulting policy set is 30 minutes.

Set the Agent Policy Set to the Empty Policy if this group is to have to effect on the policy calculations.

- E-Mail
Select any users who have been added to the E-Mail Notification list on PLUS The selected users will be sent group-based notifications.
 - Number of Computer Members
The total number of computers that are in the selected group.
 - Number of Computers assigned to the Mandatory Baseline
The total number of computers who are currently assigned to the group.
- Screen Functions
 - Reset
Resets the page back to its initial state.
 - OK
Initiates the process to save the group's changes. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
 - Cancel
Cancels the edit process and closes the group property page window.

13.2 Group Property Screen - Members

The Computer Members Group Property Page section of PLUS allows the PatchLink User the ability to edit a group. System-defined groups cannot be changed. The **Computer Members** tab of the property page contains a list of all computers which have been assigned as members of the group and the list of computers which are not a member of the group.

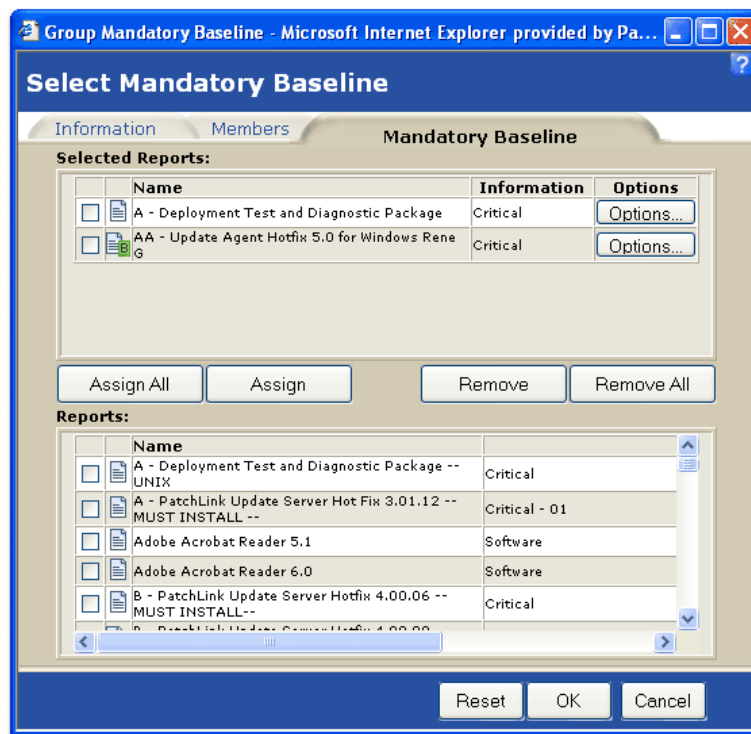


- Selected Computers
 - Operating System
The operating system platform name. Click the  to display the list of computers for that operating system. Click  to close the list.
 - Computer Name
The name of the computer.
 - DNS Name
The DNS name assigned to the computer
 - Total Selected per OS
The total number of computers that have been selected for the operating system platform.
- Available Computers
 - Operating System
The operating system platform name. Click the  to display the list of computers for that operating system. Click  to close the list.
 - Computer Name
The name of the computer.
 - DNS Name
The DNS name assigned to the computer
 - Total Selected per OS
The total number of computers that have not been selected for the operating system platform.

- Screen Functions
 - Assign All
Assigns all available computers to the group.
 - Assign
Assigns all available computers to the group.
 - Remove
Removes the selected computers from the group.
 - Remove All
Removes all selected computers from the group.
 - Cancel
Cancels the edit process and closes the group property page window.
 - Reset
Resets the page back to its initial state.
 - OK
Initiates the process to save the group (or the group's changes). If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
 - Cancel
Cancels the edit process and closes the group property page window.

13.3 Group Property Screen –Mandatory Baseline

The Group Property Page section of PLUS allows the **PatchLink User** the ability to edit a group, system-defined groups cannot be changed. The **Mandatory Baseline** tab of the property page contains the lists of selected and available Vulnerabilities and Locally-created Distribution Packages for the group's baseline.



- Selected Baseline Items
 - Baseline Item Name
The name of the vulnerability or package.
 - Baseline Item Type
This is either a Vulnerability or a Distribution Package.
 - Information
This contains information about the operating systems for the package or the impact for a vulnerability.
 - Click the Options button to display a screen with the deployment options and information about the item.

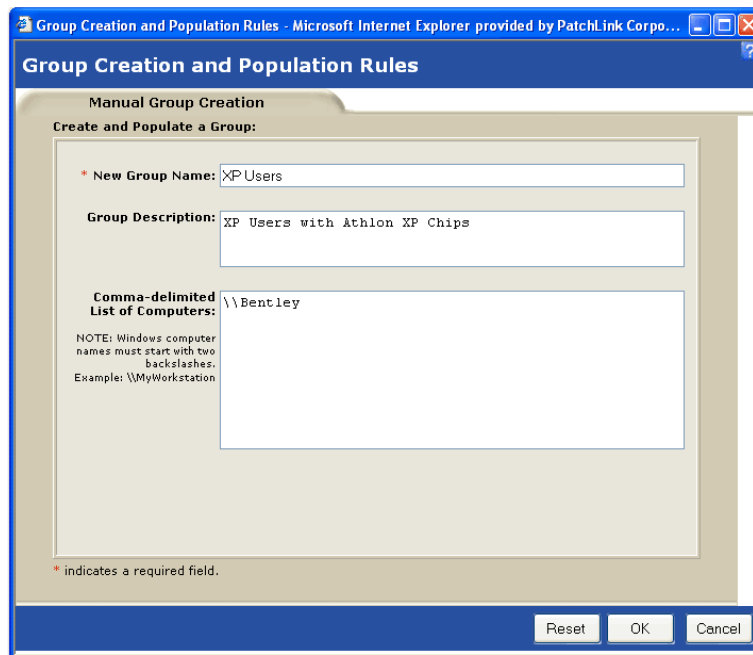


Sequential (default) indicates that only N (defaulted to 25) number of computers may perform this deployment at any given moment. The other computers will get the deployment, but it is on a first come first serve basis.

Parallel, or all computers may receive the deployment as they connect up to PLUS to get their tasks.

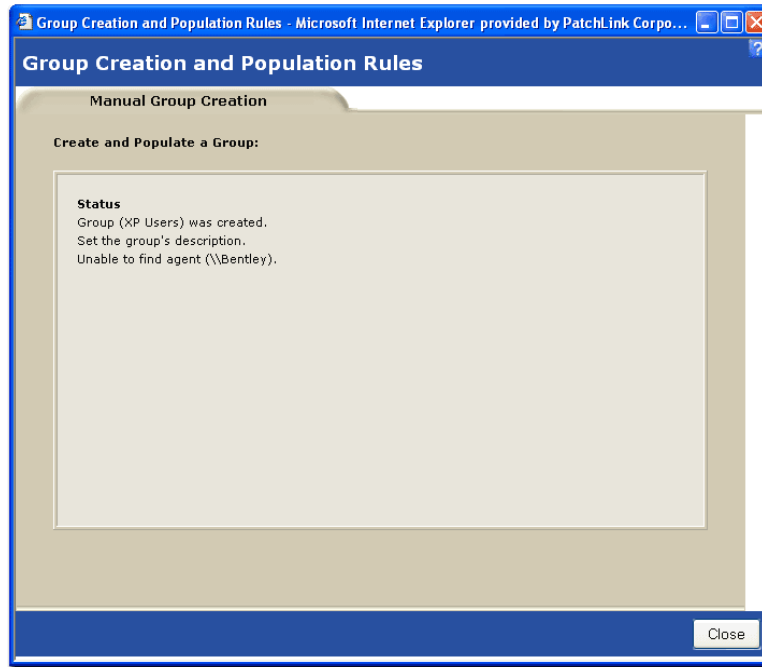
- Available Computers
 - Baseline Item Name
The name of the vulnerability or package.
 - Baseline Item Type
This is either a Vulnerability or a Distribution Package.
 - Information
This contains information about the operating systems for the package or the impact for a vulnerability.
- Screen Functions
 - Assign All
Assigns all available vulnerabilities and packages to the group.
 - Assign
Assigns all available vulnerabilities and packages to the group.

- **Remove**
Removes the selected vulnerabilities and packages from the group.
 - **Remove All**
Removes all selected vulnerabilities and packages from the group.
 - **Reset**
Resets the page back to its initial state.
 - **OK**
Initiates the process to save the group (or the group's changes). If a Mandatory Baseline item has been edited which requires a license to agree prior to the saving of the group, a license agreement page will be displayed. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
 - **Cancel**
Cancels the edit process and closes the group property page window.
 - **Options**
Displays a window with the deployment options for the item.
- **Edit**
Selecting a group and clicking on this button will bring up the Group Property page with this group's information allowing the group to be changed.
 - **Rules**
Clicking this button will bring up the Manual Group Creation and Population Rules property page.



Define a new group by filling in a new group's name and description. The group will be auto-populated by adding in a comma-separated list of computer names.

Clicking the OK button initializes the Manual Group Creation status screen.



Upon clicking the Close button of the Manual Group Creation status screen, the **Groups Homepage** is automatically refreshed showing the newly created computer group.

14. Users

Home | Vulnerabilities | Inventory | Packages | Computers | Groups | **Users** | Reports | Options | Help

The User Management section of PLUS allows the PatchLink Administrator the ability to manage who has access to log in to PLUS and once they are logged in, what sections and functions they can access, and what computers and groups they can perform those functions on.

14.1 PatchLink Users

This displays the users who have the ability to log in to PLUS and what User Role each user has.

Users						Total Users: 7
	User Name	Role	Full Name	First Logged On	Last Logged On	
☐	Administrator	Administrator		6/17/2003 7:14:09 AM	7/18/2003 7:44:39 AM	
☐	BILLW	Administrator	Bill Wesson	6/6/2003 7:04:25 AM	8/1/2003 4:01:45 PM	
☐	J. Bentley	Administrator	Joseph J. Bentley			
☐	mike	Loser Role	Michael	7/21/2003 4:11:59 PM	7/22/2003 10:32:24 AM	
☐	PatchLink	Administrator	PatchLink	6/5/2003 3:44:17 PM	8/4/2003 4:38:43 PM	
☐	SUPPORT1\pdaddy	Administrator		6/16/2003 10:19:41 AM	8/4/2003 5:39:35 PM	
☐	SUPPORT1\reneg	Administrator		6/22/2003 11:35:00 PM	7/11/2003 7:55:10 AM	

patchlink Create Add Edit Remove Delete Export

14.2 User Information

- Username
The name a user uses to log in to PLUS with.
- Role
What user role the user is assigned.
- Full Name
The user's full name.
- First Logged On
When the user first logged on to PLUS.
- Last Logged On
When the user last logged on to PLUS.

14.3 Action Menu



- **Create**
Allows a PatchLink Administrator to create new local machine users and add them as users who have access to log on to PLUS. See [Section 15; Create a User](#) for more information.
- **Add**
Allows a PatchLink Administrator to give an existing Windows user access to log on to PLUS. See [Section 16; Add a User](#) for more information.
- **Edit**
The Edit a User Wizard allows PatchLink Administrator the ability to edit a user's information and change their user role, if needed. This page of the wizard gives an overview of the wizard's function. See [Section 17; Edit a User](#) for more information.
- **Remove**
Allows a PatchLink Administrator to remove a Windows User from being able to log on to PLUS. This does not delete the Windows user.
- **Delete**
Allows a PatchLink Administrator to remove a Windows User from being able to log on to PLUS and then delete the user from the local machine.
- **Export**
Exports the lists of uses and their information to a comma-separated value (CSV) file.

14.4 User Management Security

*The user management section of PLUS requires the **View User Management** access right. If a user does not have the correct access the access denied error message is displayed.*

*To be able to Create, Add, Edit, Remove, or Delete users within the **User Management** section of PLUS requires the **Manage Users** access right. If a user does not have the correct access, the **Create**, **Add**, **Edit**, **Remove** and **Delete** buttons are disabled.*

*To be able to export the user data to a comma-separated value (CSV) file requires the **Export User Data** access right. If a user does not have the correct access, the **Export** button is disabled.*

Contact your [PatchLink Administrator](#) for more information on [PatchLink Update Security](#).

14.5 User (Security) Roles

A User Role defines what a user can see, what they can do, and what they can perform those actions on. If a user is able to log in to PLUS but does not have any access they will not be able to view any pages, perform any functions on any groups or computers. This will literally see nothing, nor be able to do nothing. At any given time, there must be at least one user who has the Administrator User Role.

Every page, feature, function and individual action of PLUS is constrained to a series of Access Rights. Based on what Access Rights a role has defines what pages and functionality or actions the users who are assigned that role have.

By default there are four system-defined User Roles: Administrator, Manager, Operator and Guest. The PLUS Administrator can assign these roles to PatchLink users or use them as templates to create new User Roles. By default all groups and computers are added to these user roles when they are created or registered. The various roles are:

The screenshot shows the 'Users' management page in PatchLink. It features a navigation bar with links like Home, Reports, Inventory, Packages, Computers, Groups, Users, and Options. The main content area is titled 'User Management: Enabled User Roles' and includes a 'Filter By: Enabled' dropdown. Below this is a table with columns for User Role Name, Type, Access Rights, Users, Groups, and Computers. The table lists six roles: Administrator, Manager, Operator, Guest, Assistant Supervisor, and Data Verification Office. At the bottom, there are buttons for PatchLink_Help, Add, Edit, Disable, and Export.

User Role Name	Type	Access Rights	Users	Groups	Computers
Administrator	System	52	25	34	28
Manager	System	49	7	34	8
Operator	System	39	3	34	8
Guest	System	16	11	34	9
Assistant Supervisor	Custom	39	0	19	4
Data Verification Office	Custom	39	1	34	8

14.6 User Roles

- Administrator**
 Any user who is assigned this User Role is considered a PatchLink Super-User, as they have full access to everything. Users of this role are the only users who can delegate newly installed computers to other user roles.
- Manager**
 The Manager User role can manage every section of PLUS other than the Advanced Configuration Options and User Management.
- Operator**
 The Operator user role can perform all routine operations (deploy, detect, export).
- Guest**
 The Guest user role can access all of the pages but perform no functionality on what they see.

-  Custom
The custom user role is a role that is defined by a PatchLink Administrator. The PatchLink Administrator defines access rights, groups and computers that these roles have access to.
-  Disabled Custom
This customer user role has been disabled. Any users who are assigned this role do not have will not have any access to any of the PLUS sections, functions, computers or groups.

14.7 User Role List

- User Role Name
The name of the user role.
- Type
System or Custom, based on who created the role.
- Access Rights
The number of access rights assigned to the user role.
- Users
The number of users assigned this user role.
- Groups
The number of groups assigned to the user role.
- Computers
The number of computers assigned to the user role.

14.8 Action Menu



- Add
The Role Property pages allow the PatchLink Administrator to create or edit a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use this page to specify basic role information. See [Section 18; Add a Role Wizard](#) for more information.
- Enable
Allows a PatchLink Administrator to enable an existing (non-system) user role.

- **Edit**
Allows a PatchLink Administrator to change an existing (non-system) user role.
See [Section 19; Edit a Role](#) for more information.
- **Disable**
Allows a PatchLink Administrator to disable an existing (non-system) user role.
- **Remove**
Allows a PatchLink Administrator to delete an existing (non-system) disabled user role.
- **Export**
Exports the lists of user roles and their information to a comma-separated value (CSV) file.

14.9 User Roles Security

*The user roles section of PLUS requires the **View User Management** access right. If a user does not have the correct access, the access denied error message is displayed.*

*To be able to Add, Edit, or Remove user roles within the User Role section of PLUS requires the **Manage Users** access right. If a user does not have the correct access, the **Add**, **Edit**, and **Remove** buttons are disabled.*

*To be able to export the user role data to a comma-separated value (CSV) file requires the **Export User Data** access right. If a user does not have the correct access, the **Export** button is disabled.*

Contact your PatchLink Administrator for more information on [Patchlink Update Security](#).

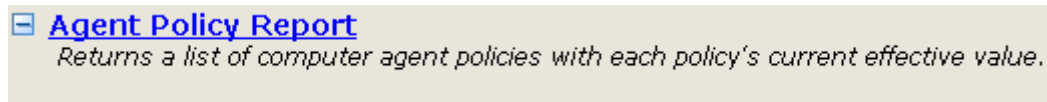
15. Reports

[Home](#) | [Vulnerabilities](#) | [Inventory](#) | [Packages](#) | [Computers](#) | [Groups](#) | [Users](#) | [Reports](#) | [Options](#) | [Help](#)

The **Reports** link in the main menu launches the first **Application Reporting** window, which contains various printable and exportable report selections to provide a system-wide view of your network's patch status.



Click on the next to each report to see a general description of the data each report handles.



When you click on the report hyperlink, a second Application Reporting window opens where you can specify the reporting **Parameters** and generate your report.

15.1 Application Reporting Parameters

The following list of report parameters encompasses all available parameters across all reports.

Computers

Allows the user to select from a list of one or more computers. The Search feature allows the user to search by Computer Name.

Groups

Allows the user to select from a list of one or more groups of computers. The result will be the union of all computers in the group(s) selected. The Search feature allows the user to search by Group Name.

Deployments

Allows the user to select from a list of deployment names. The Search feature allows the user to search by Deployment Name.

Vulnerabilities

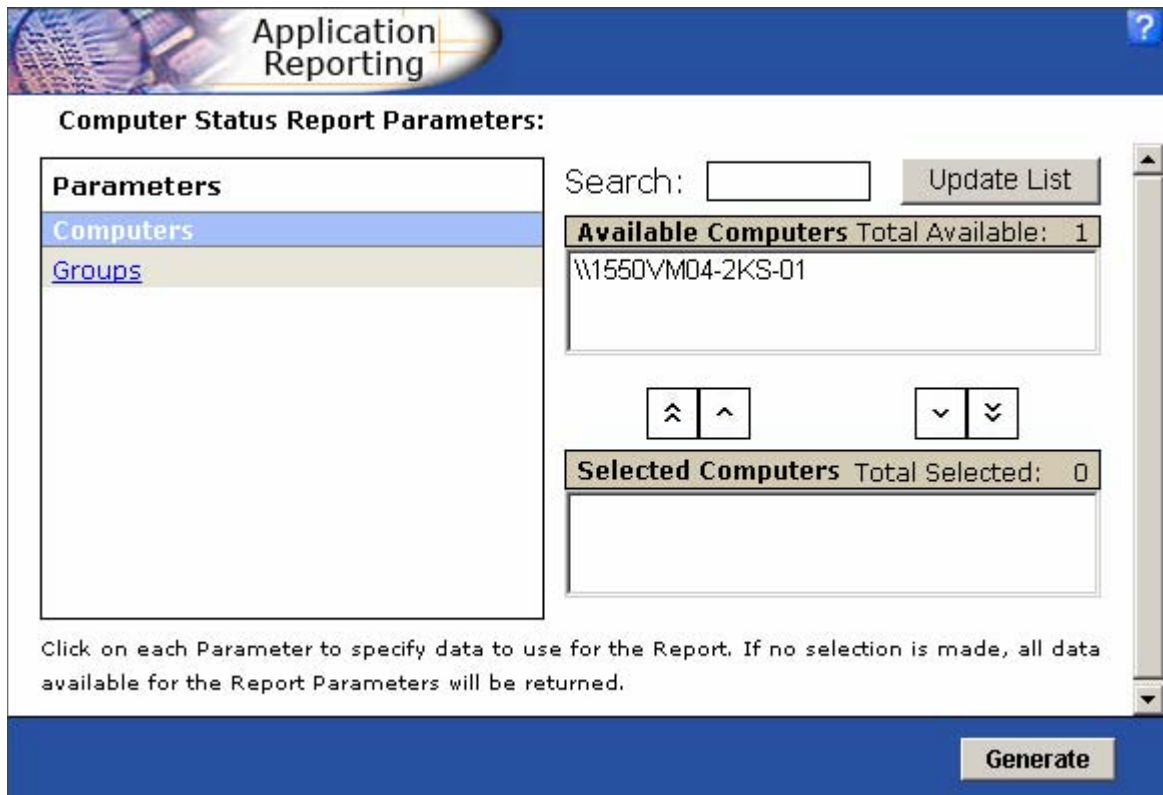
Allows the user to select from a list of all available vulnerabilities. The Search feature allows the user to search by Vulnerability Name and/or CVE/CAN.

Date Range

Allows the user to specify a date range that will be compared to the Deployment start date. The user has the option of displaying the time in 12 or 24 hour format and as PLUS local time or UTC time.

Packages

Allows the user to select from a list of all available packages. The Search feature allows the user to search by Package Name.



Application Reporting

Computer Status Report Parameters:

Parameters	Search:	Update List
Computers	Available Computers Total Available: 1 W1550VM04-2KS-01	
Groups	⬆ ⬆ ⬇ ⬇ Selected Computers Total Selected: 0	

Click on each Parameter to specify data to use for the Report. If no selection is made, all data available for the Report Parameters will be returned.

Generate

Report Parameters are defined by selecting an option in the Parameters list then narrowing the report data using the **Available** data list that appears in the right side of the Application Reporting window. To expedite the selection of data, a **Search** feature is available for each Parameter. Simply enter the search text, e.g. Computer, Group, Vulnerability, or Package Name, depending on the Parameter being defined, in the Search field and click the

Update List

button. The desired information appears in the grid beneath the Search field.

Search:

Available Vulnerabilities	Total Available: 5
Adobe Acrobat Reader 5.1	
Adobe Acrobat Reader 6.0	
Adobe Acrobat Reader 6.0.1	
Adobe Acrobat Reader 6.0.1 (Korean)	
Adobe Acrobat Reader 6.0.2 update	

To move items into the **Selected** data list from the Available data list, highlight the items and click the  button. Move all Available data to the Selected data list using the  button. Items can be removed from the Selected data list using the reverse arrows: use the  button to remove one or more selected items and the  button to remove the entire list.

Once the report data has been defined, the report is created by clicking the button. You may choose not to define any Parameters; in this case, all applicable data for the report Parameters will be returned.

Application Reporting – Generated Report

Reports can be sorted by the data in any column by clicking the column header; sort order switches between ascending and descending order. For reports that generate date range data, the user can choose to display the PLUS date/time information in either local or UTC (also known as GMT) time.

Display dates as:
☒ PLUS Local Time ☐ PLUS UTC Time

An HTML version of the report can be quickly printed using the **View Printable** option and reports can be exported in the following formats:

- Comma Separated Values (CSV)
- Microsoft Excel Worksheet (XLS)
- XML Document

Comma Separated Values (CSV) ▼

Comma Separated Values (CSV)

Microsoft Excel Worksheet (XLS)

XML Document

☒ Trusted sites

15.2 Application Reporting Security

The Application Reporting section of PLUS requires the **Manage User-Based Reports** or the **Manage Administrative Reports** access right. If a user is not assigned one of these access rights, the Reports link in the main menu is not functional and an "access denied" error message is returned if the user attempts to manually load the Reports page by entering the URL directly.

- **Manage User-Based Reports** – User can run reports only for those computers and groups specifically assigned to the user in the User Roles section. Computers and Groups not assigned to the user do not appear on the Parameter selection page.
- **Manage Administrative Reports** – User can run reports for all computers and groups on the network, regardless of user role and computer or group assignments.

Example – Generate a Computer Status Report

To generate a Computer Status Report for agents in the Windows 2000 group, perform the following steps:

1. Select the Reports menu option from the main menu of the PatchLink Update Server Web interface.



2. On the first Application Reporting window, click the hyperlink for **Computer Status Report**. The Application Reporting window for Computer Status Report Parameters opens with the Groups parameter selected by default.
3. In the right side of the window, scroll through the Available Groups section to find the group *Win2K*.

Available Groups	Total Available: 12
Win2K	☒
Win2K3	☐
Win95	☐
Win98	☐

4. Select the Win2K group and click the ☒ button to transfer the selection to the Selected Groups pane below.

Selected Groups	Total Selected: 1
Win2K	

- Click the Generate button. The Computer Status Report appears.

Application Reporting

Computer Status Report Report created: 8/16/2004 4:33:00 PM

ComputerName	DNSName	IPAddress	OperatingSystemName	OSBuildNo	ServicePack	AgentVersion
\\1550VM04-2KS-01	1550vm04-2ks-01.engineering.patchlink.com	192.168.1.210	Microsoft Windows 2000 Server	2195	Service Pack 4	6.0.1.65

Export Comma Separated Values (CSV) View Printable Close

- To export the report, select a format for the exported file from the drop-down list next to the Export button, then click Export. Alternately, to print the report, click the View Printable option then select File > Print.

15.3 Available Reports

Following is a list of available reports. Definitions for output data are provided where the meaning is not readily apparent.

Agent Policy Report

The Agent Policy Report returns a list of Agent Policies and their current effective value for the selected computers. Available Parameters for this report are *Computers* and *Groups*.

ComputerName	PolicyName	CurrentValue	PolicyDesc
\\1550VM04-2KS-01	IntervalType	S	Type of time period. S=Seconds,M=Minutes,H=Hours
\\1550VM04-2KS-01	Interval	300	Number of time periods that agent should check host for Tasklist.
\\1550VM04-2KS-01	Start	12:00 AM	The time of day the agent should start running and checking for work to do (GMT).
\\1550VM04-2KS-01	End	12:00 AM	The time of day the agent should stop running and checking for work to do (GMT).
\\1550VM04-2KS-01	DeployTimeout	2	The timeout value for deployment notifications.
\\1550VM04-2KS-01	SnoozeDuration	60	The snooze duration for deployment notifications.
\\1550VM04-2KS-01	SnoozeLimit	15	The number of times a deployment notification can be snoozed.
\\1550VM04-2KS-01	RebootTimeout	2	The timeout value for reboot notifications.
\\1550VM04-2KS-01	RebootDuration	60	The snooze duration for reboot notifications.
\\1550VM04-2KS-01	RebootLimit	15	The number of times a reboot notification can be snoozed.
\\1550VM04-2KS-01	DagentMode	0	0 = Slow, 1 = Fast on install only, 2 = Fast

Computer Status Report

The Computer Status Report returns the current state of remediation for a specified computer, list of computers, computers in a group, or computers in a list of groups. Available Parameters for this report are *Computers* and *Groups*.

ComputerName	DNSName	IPAddress	OperatingSystemName	OSBuildNo
\\1550VM04-2KS-01	1550vm04-2ks-01.engineering.patchlink.com	192.168.1.210	Microsoft Windows 2000 Server	2195

ServicePack	AgentVersion	LastContactDate	PatchableStatus	GroupList
Service Pack 4	6.0.1.65	8/17/2004 7:57:26 PM	Clean	Win2K

Output definitions:

Patchable Status refers to the reboot status of the agent. Values are:

- o Clean – the agent is ready to receive a patch
- o Dirty – the agent requires a reboot before receiving the next patch
- o Q-Chain – the agent is waiting for a Q-chain deployment

Group List – A delimited list of groups the agent belongs to

Deployment Detail Report

The Deployment Detail Report returns a detailed list of computers by selected deployments. Available Parameters for this report are *Deployments*, *Vulnerabilities*, and *Date Range*. If a selected Vulnerability has no associated deployment, it will not appear in the report.

DeploymentName	VulnerabilityName	ComputerName
Deployment of Test Pkg 2 MS04-003 832483 Buffer Overrun in MDAC Function MDAC 2.7 SP1-a (Win2K,WinXP,Win2K3,WinNT)	MS04-003 832483 Buffer Overrun in MDAC Function MDAC 2.7 SP1	\\1550VM04-2KS-01

DeploymentStatus	DeploymentDate	InstallDate	VulnerabilityStatus	DateLastVerified
Package Being Cached	8/19/2004 6:46:00 AM	8/19/2004 1:46:00 PM	Not Patched	8/19/2004 6:44:06 PM

Deployment Summary Report

The Deployment Summary Report returns an analysis for a selected list of deployments. Available Parameters for this report are *Deployments*, *Vulnerabilities*, and *Date Range*. If a selected Vulnerability has no associated deployment, it will not appear in the report.

<u>DeploymentName</u>	<u>VulnerabilityName</u>	<u>TotalDeployed</u>	<u>TotalSuccessful</u>
Deployment of Test Pkg Deployment Test and Diagnostic Package (WinXP,Win2K,Win95,Win98,WinME,WinNT,Win2K3)	A - Deployment Test and Diagnostic Package	1	0

<u>TotalInProgress</u>	<u>TotalFailed</u>	<u>TotalDisabled</u>	<u>TotalPatched</u>	<u>PercentSuccess</u>	<u>PercentFailure</u>
0	0	0	0	0	0

Mandatory Baseline Detail Report

The Mandatory Baseline Detail Report returns a detailed list of computers by mandatory baseline packages/vulnerabilities. Available Parameters for this report are *Computers* and *Groups*.

<u>ComputerName</u>	<u>GroupName</u>	<u>PackageName</u>	<u>VulnerabilityStatus</u>	<u>DeploymentStatus</u>
\\1550VM04-2KS-01	Win2K	Adobe Acrobat Reader 6.0.1	Detecting	Package Being Cached
\\1550VM04-2KS-01	Win2K	Deployment Test and Diagnostic Package	Not Patched	Package Being Cached

<u>DateDeployed</u>	<u>DateInstalled</u>	<u>DateLastVerified</u>
8/19/2004 9:46:35 PM	8/19/2004 9:46:35 PM	
8/19/2004 6:45:00 AM		8/19/2004 10:09:36 PM

Mandatory Baseline Summary Report

The Mandatory Baseline Summary Report returns an analysis for a selected list of mandatory baseline packages/vulnerabilities. Available Parameters for this report are *Computers* and *Groups*.

<u>PackageName</u>	<u>TotalDeployed</u>	<u>TotalSuccessful</u>	<u>TotalInProgress</u>	<u>TotalFailed</u>	<u>PercentSuccess</u>	<u>PercentFailure</u>
Adobe Acrobat Reader 6.0.1	1	0	0	0	0	0
Deployment Test and Diagnostic Package	1	0	0	0	0	0

Package Compliance Detail

The Package Compliance Detail Report returns a detailed list by package and computer with patch and deployment status for all applicable computers. Available Parameters for this report are *Computers*, *Groups*, and *Packages*. If a selected Package has no associated deployment, it will not appear in the report.

PackageName	ComputerName	VulnerabilityStatus	DateLastVerified	DeploymentName
Adobe Acrobat Reader 6.0.1	\\1550VM04-2KS-01	Not Patched	8/19/2004 10:14:24 PM	Deployment of Adobe Acrobat Reader 6.0.1
MS04-003 832483 Buffer Overrun in MDAC Function MDAC 2.7 SP1-a	\\1550VM04-2KS-01	Not Patched	8/19/2004 10:14:27 PM	Deployment of Test Pkg 2 MS04-003 832483 Buffer Overrun in MDAC Function MDAC 2.7 SP1-a (Win2K,WinXP,Win2K3,WinNT)

DeploymentStatus	DateDeployed	DateInstalled	DateScheduled
Package Being Cached	8/19/2004 9:46:35 PM	8/19/2004 9:46:35 PM	
Package Being Cached	8/19/2004 6:46:00 AM		

Package Compliance Summary

The Package Compliance Summary Report returns information on the overall patch and deployment status of a specific package. Available Parameters for this report are *Computers*, *Groups*, and *Packages*. If a selected Package has no associated deployment, it will not appear in the report.

PackageName	TotalComputers	ApplicableComputers	ComputersDetecting	ComputersPatched	NotPatchedNotScheduled
Adobe Acrobat Reader 5.1	1	1	0	0	1
Adobe Acrobat Reader 6.0	1	1	0	0	1

NotPatchedScheduled	DeploymentsCompleted	DeploymentsFailed	DeploymentsInProgress
0	0	0	0
0	0	0	0

Output definitions:

Total Computers

Count of computers applicable to the selected report criteria.

Applicable Computers

Count of computers applicable to the vulnerability.

Vulnerability Analysis Report

The Vulnerability Analysis Report returns the current state of remediation for a specified list of vulnerabilities, computers and groups. Available Parameters for this report are *Computers*, *Groups*, and *Vulnerabilities*. If a selected Vulnerability has no associated deployment, it will not appear in the report.

<u>VulnerabilityName</u>	<u>TotalComputers</u>	<u>ApplicableComputers</u>
A - Deployment Test and Diagnostic Package	1	1
Adobe Acrobat Reader 6.0.1	1	1
MS04-003 832483 Buffer Overrun in MDAC Function MDAC 2.7 SP1	1	1

<u>ComputersDetecting</u>	<u>ComputersPatched</u>	<u>NotPatched</u>	<u>PctPatched</u>
0	0	1	0
0	0	1	0
0	0	1	0

Output definitions:

Total Computers

Count of computers applicable to the selected report criteria.

Applicable Computers

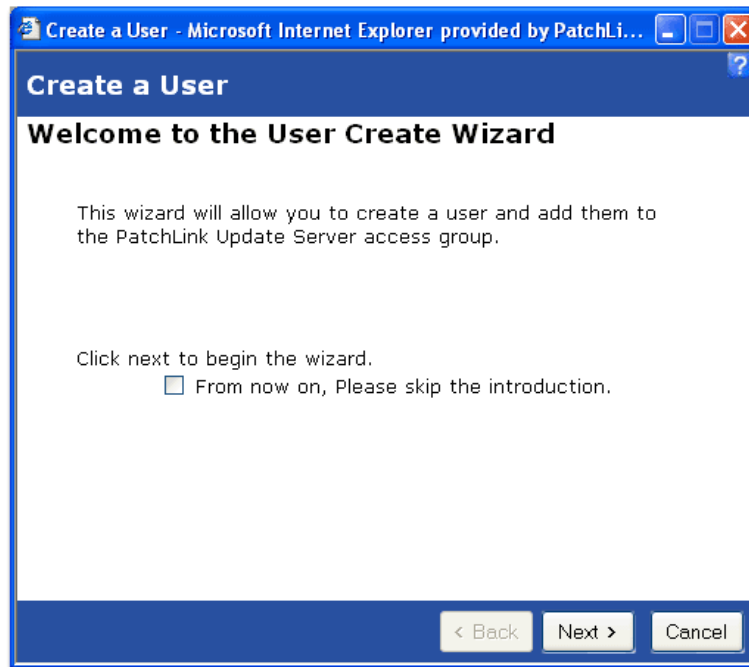
Count of computers applicable to the vulnerability.

16. Create a User Wizard

The **Create a User** Wizard allows PatchLink Administrator the ability to create local Windows users and give them access to PLUS. Enter basic information required to create the user.

16.1 Welcome

From the **Users** homepage, Users Tab, click on the **Create** button on the Action Menu. The Welcome Screen appears.



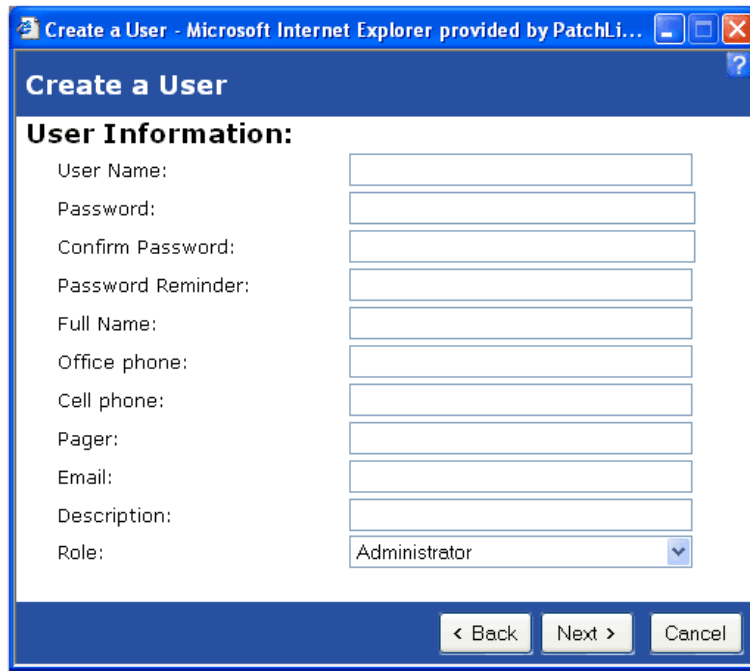
16.2 Screen Functions

- **Skip**
The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Create a User Wizard is initialized.
- **Back**
The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.
- **Next**
The **Next** button initializes the wizard's next screen.
- **Cancel**
The **Cancel** button closes the wizard.

Click the **Next** button to enter User Information.

16.3 User Information

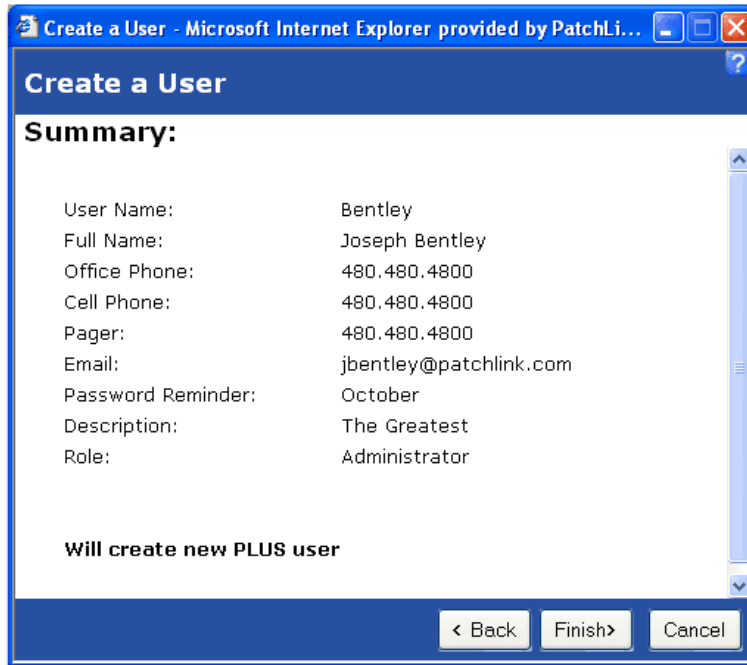
Enter User Information into the appropriate fields and select their **Role** from the dropdown menu. A User Role defines what a user can see, what they can do, and what they can perform those actions on. If a user is able to log in to PLUS, but does not have any access, they will not be able to view any pages, perform any actions or functions on any groups or computers. This is literally see nothing, nor be able to do nothing. At any given time, there must be at least one user who is assigned to the Administrator User Role.



After entering in all User information, click the **Next** button to verify a summary of the data before the user is created.

16.4 Summary

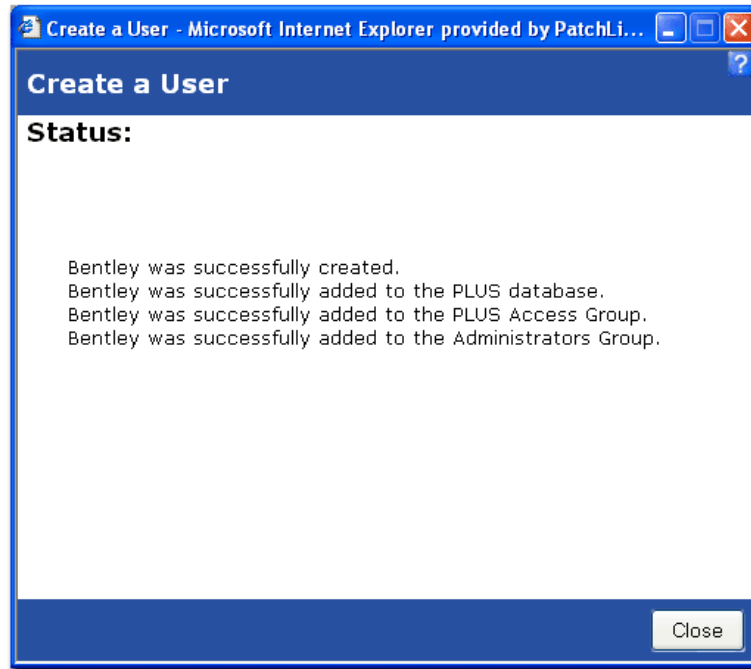
Verify the accuracy of all entered User information. Click the **Back** button to initialize the previous User Information screen and edit user information. Click the **Next** button to initialize the creation of the user and to view the Status screen.



Create a User	
Summary:	
User Name:	Bentley
Full Name:	Joseph Bentley
Office Phone:	480.480.4800
Cell Phone:	480.480.4800
Pager:	480.480.4800
Email:	jbentley@patchlink.com
Password Reminder:	October
Description:	The Greatest
Role:	Administrator
 Will create new PLUS user	
< Back Finish> Cancel	

16.5 Status

The user was created and added to the PatchLink Update Server Access Group.



If the user was given access to a user role which has the Manage Users Access Right, they will also be added to the Windows Administrators group on the local PLUS computer.

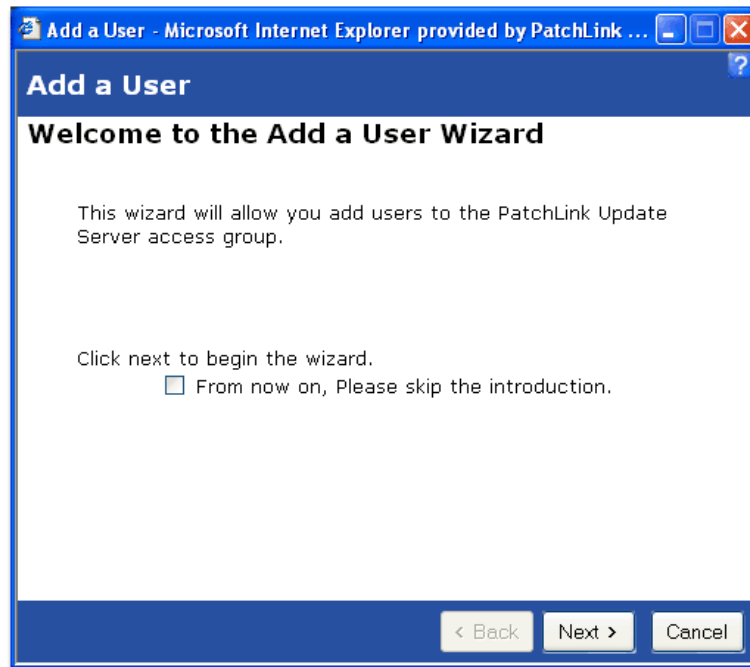
Upon Closure of the Status window, the newly created user will appear on the Users homepage after it is refreshed.

17. Add a User Wizard

The **Add a User** Wizard allows a PatchLink Administrator to give an existing Windows user access to log on to PLUS.

17.1 Welcome

From the **Users** homepage, Users Tab, click on the **Add** button on the Action Menu. The Welcome Screen appears.



17.2 Screen Functions

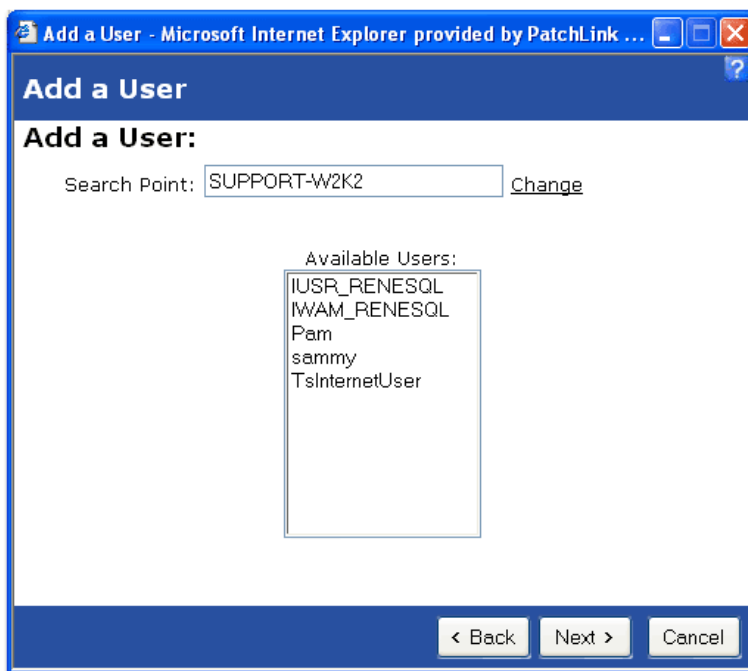
- **Skip**
The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Add a User Wizard is initialized.
- **Back**
The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.
- **Next**
The **Next** button initializes the wizard's next screen.
- **Cancel**
The **Cancel** button closes the wizard.

Click the **Next** button to enter User Information.

17.3 Add

Displayed are a list of users that are available (from your Created Users) to be added to the PatchLink Update Server Access Group.

Note: The Microsoft IIS Web server software does not support the entering of user names or passwords in languages (Korean, Kanji, etc.) that require Unicode characters. Since the PLUS patch management software uses Microsoft IIS as its Web server, end-users cannot enter usernames and passwords in Unicode to log on to the PLUS management website.

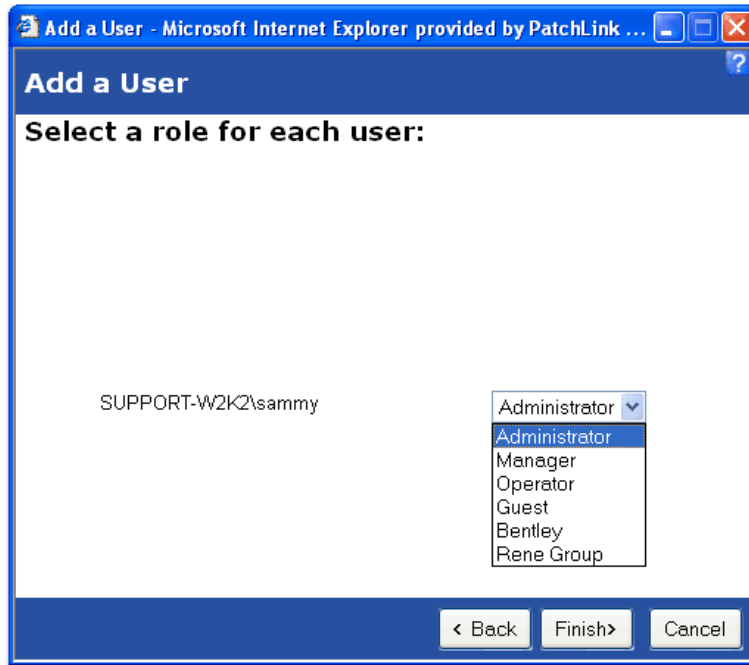


- **Search Point: Change**
The default location to check for users is the name of the computer where the PatchLink Update Server is installed on to. To change this, enter in the new search location in to the Search Point field and click on the Change hyperlink.
- **Available Users: Select**
To select a user simply click on the user's name. To select multiple users, hold the **Ctrl** (control) key down and click on the user names.

Click the **Next** button to initialize the **Roles** screen.

17.4 Select a Role

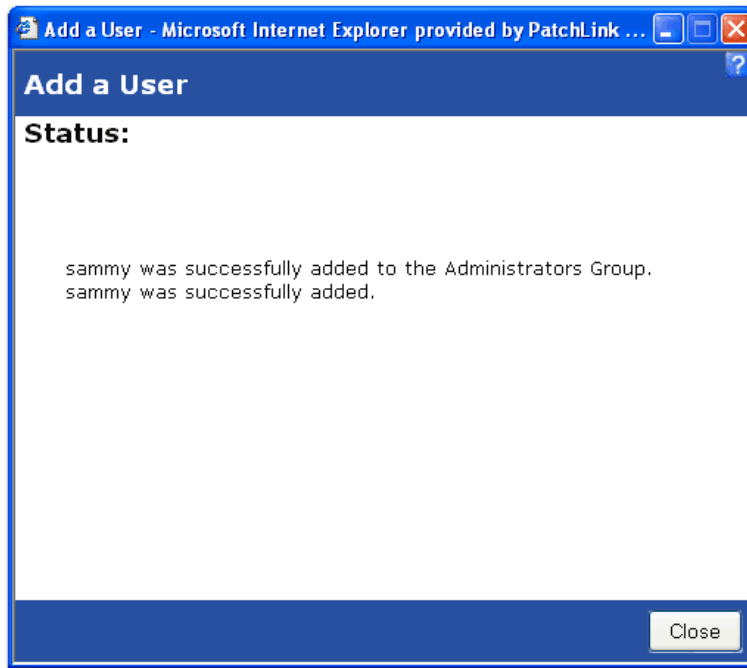
This screen displays the available user roles to choose. The selected role will be assigned to the user.



Select a User Role and click the **Finish** button.

17.5 Status

The status screen appears verifying the addition.



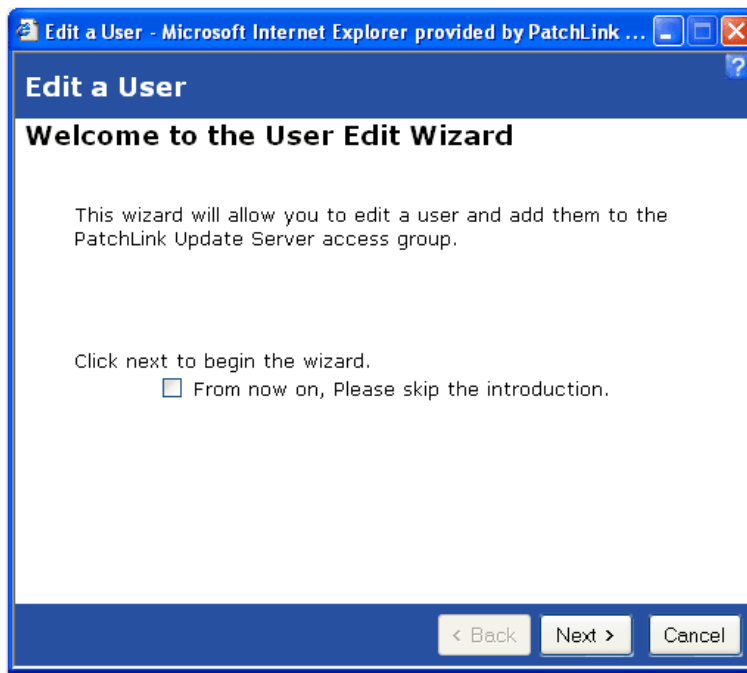
Upon clicking on the close button, the User screen is automatically refreshed with the User addition.

18. Edit a User Wizard

The **Edit a User Wizard** allows PatchLink Administrator the ability to edit a user's information and change their user role, if needed.

18.1 Welcome

From the **Users** homepage, Users Tab, select a User that you wish to edit by clicking in the checkbox next to the item and click on the **Edit** button on the Action Menu. The Welcome Screen appears.



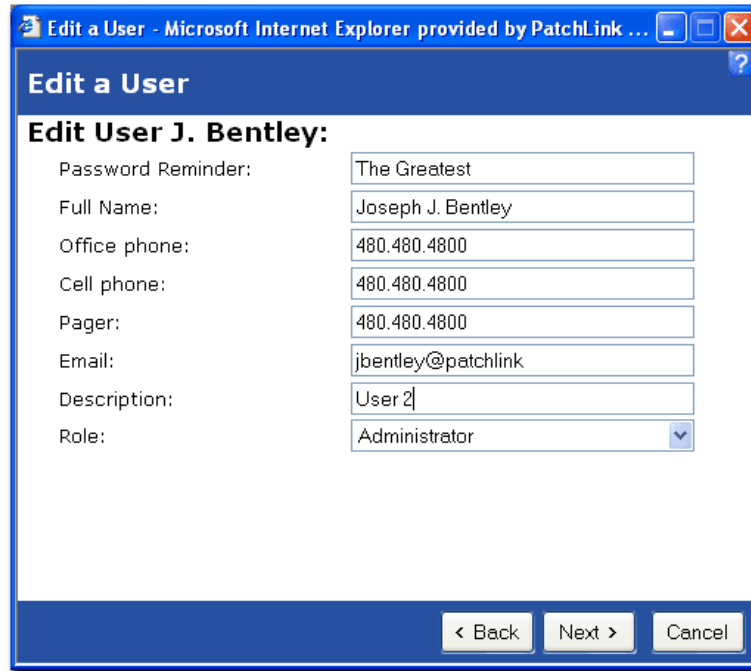
18.2 Screen Functions

- **Skip**
The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Edit a User Wizard is initialized.
- **Back**
The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.
- **Next**
The **Next** button initializes the wizard's next screen.
- **Cancel**
The **Cancel** button closes the wizard.

Click the Next button to initialize the **Edit User** screen.

18.3 Edit Information

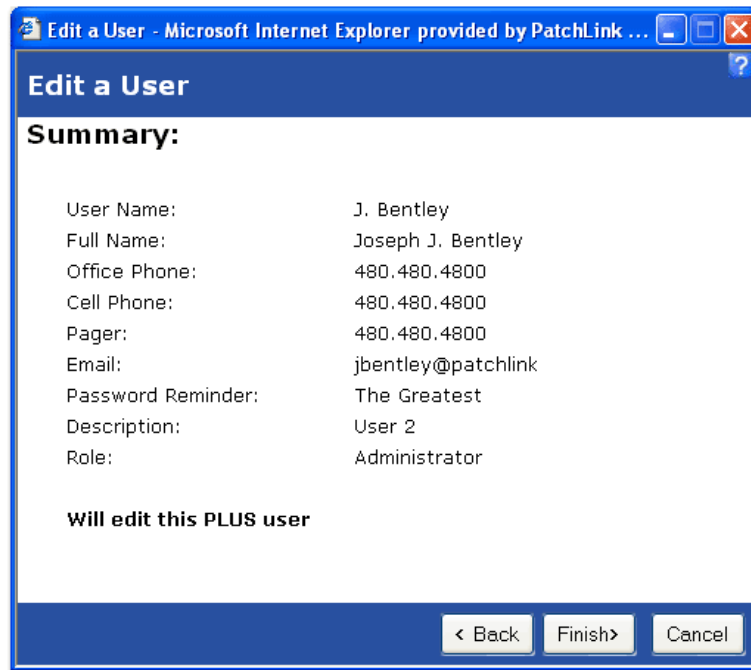
Displayed are the fields in which you entered information when you created a user.



Edit information and click the **Next** button.

18.4 Summary

Verify the accuracy of all entered User information. Click the **Back** button to initialize the previous Edit User Information screen and edit user information. Click the **Next** button to initialize the edit of the user and to view the Status screen.



Edit a User

Summary:

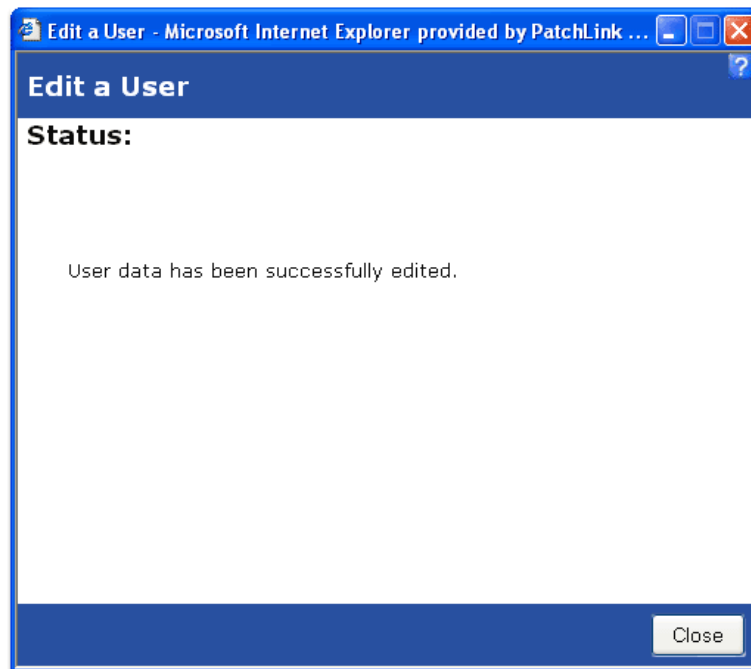
User Name: J. Bentley
 Full Name: Joseph J. Bentley
 Office Phone: 480.480.4800
 Cell Phone: 480.480.4800
 Pager: 480.480.4800
 Email: jbentley@patchlink
 Password Reminder: The Greatest
 Description: User 2
 Role: Administrator

Will edit this PLUS user

< Back Finish> Cancel

18.5 Status

The status screen appears verifying the edit.



Edit a User

Status:

User data has been successfully edited.

Close

Upon Closure of the Status window, the newly edited user information will appear on the Users homepage item after it is refreshed and viewed.

19. Add a Role Wizard

The Role Property pages allow the PatchLink Administrator to create a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Role Information** screen to specify basic role information.

19.1 Add a Role

From the Users homepage, Roles Tab, Click on the Add button on the Action Menu to initialize the **Add a Role** wizard.

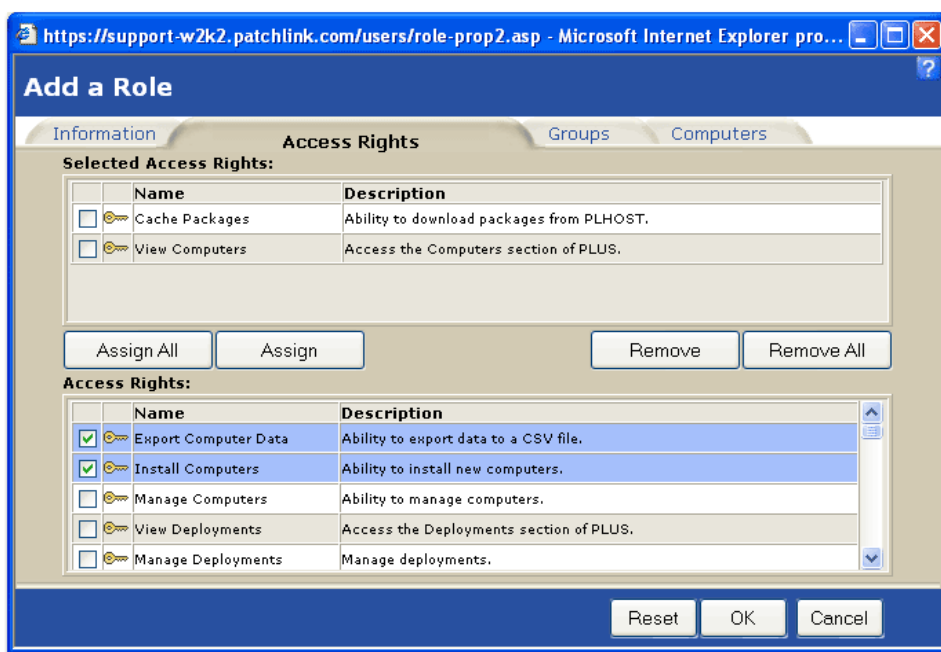
- Role Information
 - Name
Enter the name of the user role to be created or that of the role being edited.
 - Description
Enter the description of the user role.
 - Role Template
When creating a role, use this to select a pre-existing system role to use as starting point for further customization. When editing a role, this will initially display "custom" to indicate that the role is not a system role. As in creating a role, use this control to set your role to one of the system templates as a starting point for further editing.

- Screen Functions
 - Access Rights Tab
Select this tab to specify this role's access rights to various PLUS functionalities.
 - Groups Tab
Select this tab to specify the groups of computers that this role may access.
 - Computers Tab
Select this tab to specify individual computers that this role may access.

Select the Access Rights Tab to initialize the Access Rights screen and assign rights.

19.2 Access Rights

The Role Property screens allow the PatchLink Administrator to create a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Access Rights** to specify the access rights to PLUS functionalities assigned to this user role.

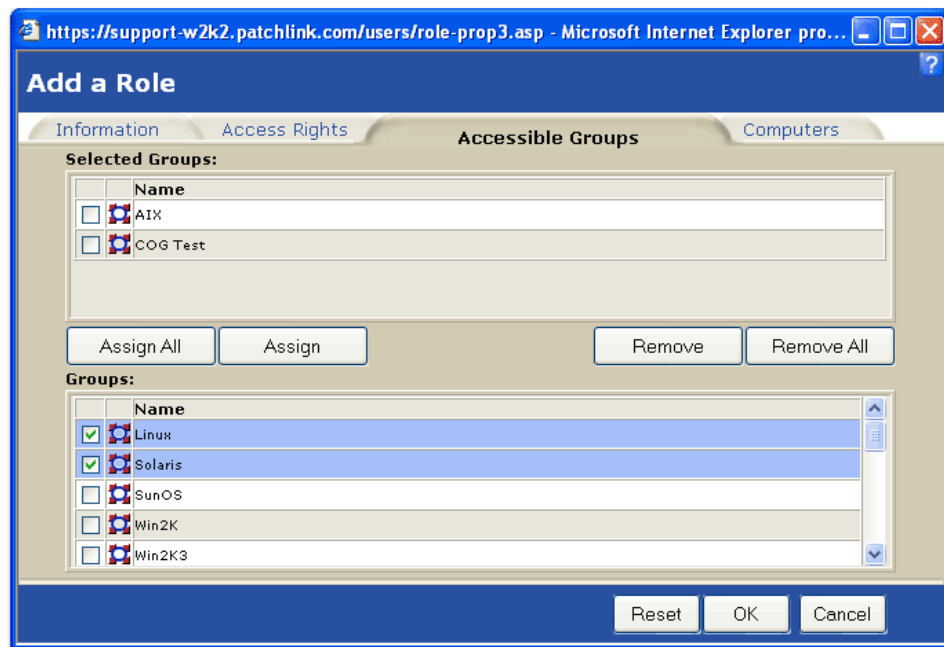


- Access Rights Information
 - Selected Access Rights
Select or Edit from the list of access rights that have been assigned to this user role.
 - Access Rights
A list of all the access rights that can be assigned to a user role. Scroll through and click in the checkbox next to the desired right(s) to initialize and click the **Assign** button. The system populates the **Selected Access Rights** window with your selections. Use the **Assign All** button to populate the **Selected Access Rights** with ALL rights from the **Access Rights** window.

- Screen Functions
 - Assign All
Click to assign all available access rights to the user role.
 - Assign
After selecting any number of the access rights listed in the "Access Rights" (lower) pane, click here to assign these rights to the user role.
 - Remove
After selecting any number of the access rights listed in the "Selected Access Rights" (upper) pane, click here to remove these rights from the user role.
 - Remove All
Click to remove from the role all of the assigned access rights.
 - Information Tab
Select this tab to specify this role's basic information.
 - Groups Tab
Select this tab to specify the groups of computers that this role may access.
 - Computers Tab
Select this tab to specify individual computers that this role may access.

19.3 Accessible Groups

The Role Property screens allow the PatchLink Administrator to create a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Groups** screen to specify the groups of computers that this user role may access.

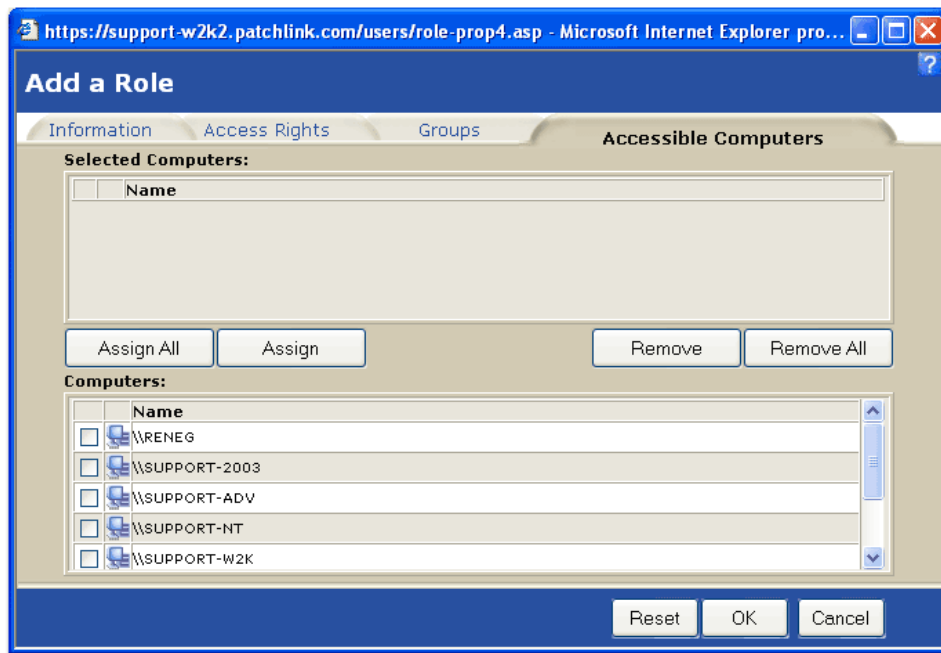


- Accessible Groups Information
 - Selected Groups
A list of the groups of computers that have been assigned to this user role.
 - Groups
A list of all the groups of computers that can be assigned to this user role.

Scroll through and click in the checkbox next to the desired group(s) to initialize and click the **Assign** button. The system populates the **Selected Groups** window with your selections. Use the **Assign All** button to populate the **Selected Groups** with ALL groups from the **Groups** window.
- Screen Functions
 - Assign All
Click to assign all available groups to the user role.
 - Assign
After selecting any number of the groups listed in the "Groups" (lower) pane, click here to assign these groups to the user role.
 - Remove
After selecting any number of the groups listed in the "Selected Groups" (upper) pane, click here to remove these groups from the user role.
 - Remove All
Click here to remove from the role all of the assigned groups.
 - Information Tab
Select this tab to specify this role's basic information.
 - Access Rights Tab
Select this tab to specify this role's access rights to PLUS functionalities.
 - Computers Tab
Select this tab to specify individual computers that this role may access.

19.4 Accessible Computers

The Role Property screens allow the PatchLink Administrator to create or edit a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Computers** to specify the individual computers that this user role may access.



- Accessible Computers Information

- Selected Computers

A list of all the computers that have been assigned to this user role.

- Computers

A list of all the computers that can be assigned to this user role.

Scroll through and click in the checkbox next to the desired computer(s) to initialize and click the **Assign** button. The system populates the **Selected Computers** window with your selections. Use the **Assign All** button to populate the **Selected Computers** with ALL computers from the **Computers** window.

- Screen Functions

- Assign All

Click to assign all available computers to the user role.

- Assign

After selecting any number of the computers listed in the "Computers" (lower) pane, click here to assign these computers to the user role.

- Remove

After selecting any number of the computers listed in the "Selected Computers" (upper) pane, click here to remove these computers from the user role.

- Remove All

Click here to remove from the role all of the assigned computers.

- Information Tab

Select this tab to specify this role's basic information.

- Access Rights Tab

Select this tab to specify this role's access rights to PLUS functionalities.

- Groups Tab

Select this tab to specify the groups of computers that this role may access.

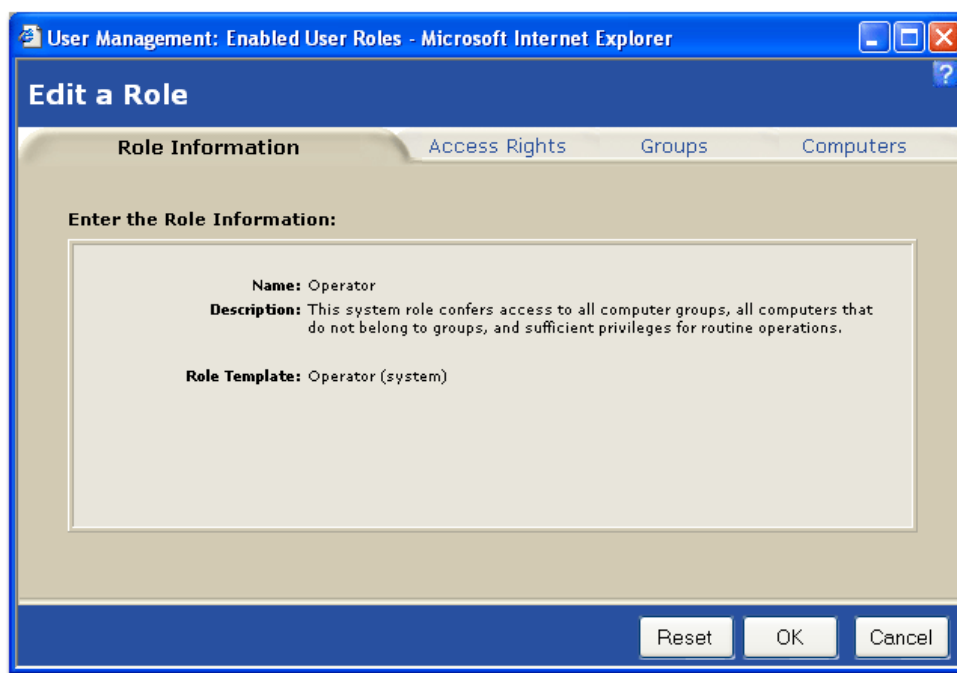
Upon closure of the Add a Role Wizard, the homepage will be refreshed with the newly entered Role.

20. Edit a Role Wizard

The Role Property screens allow the PatchLink Administrator to edit a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use this screen to view basic role information.

20.1 Edit a Role

From the Users homepage, click the Roles tab and select the Role you wish to edit by clicking in the checkbox next to it and clicking on the **Edit** button on the Action Menu. This initializes the **Edit a Role** wizard. To edit a role, you must first add one. See [Section 19; Add a Role Wizard](#) for more information.

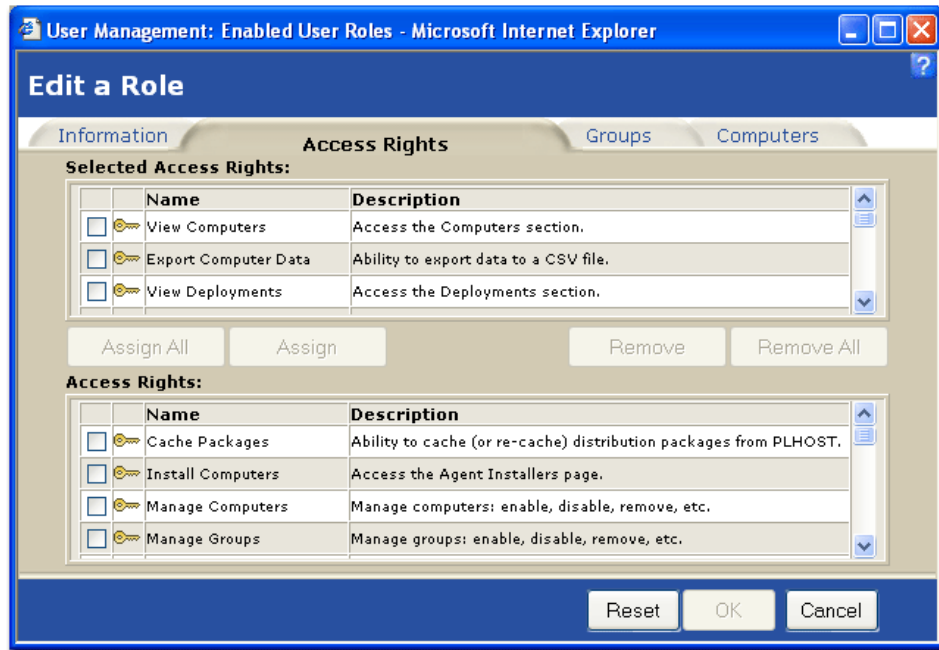


- Role Information
 - Contains the Name, Description, and Role Template information about the specific role that you chose to Edit.
- Screen Functions
 - Access Rights Tab
Select this tab to specify this role's access rights to various PLUS functionalities.
 - Groups Tab
Select this tab to specify the groups of computers that this role may access.
 - Computers Tab
Select this tab to specify individual computers that this role may access.

Select the Access Rights Tab to initialize the Access Rights screen and assign rights.

20.2 Access Rights

The Role Property screens allow the PatchLink Administrator to edit a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Access Rights** screen to specify the access rights to PLUS functionalities assigned to this user role.



- Access Rights Information
 - Selected Access Rights

Edit the list of access rights that have been assigned to this user role.
 - Access Rights

A list of all the access rights that can be assigned to a user role. Scroll through and click in the checkbox next to the desired right(s) to initialize and click the **Assign** button. The system populates the **Selected Access Rights** window with your selections. Use the **Assign All** button to populate the **Selected Access Rights** with ALL rights from the **Access Rights** window.
- Screen Functions
 - Assign All

Click to assign all available access rights to the user role.
 - Assign

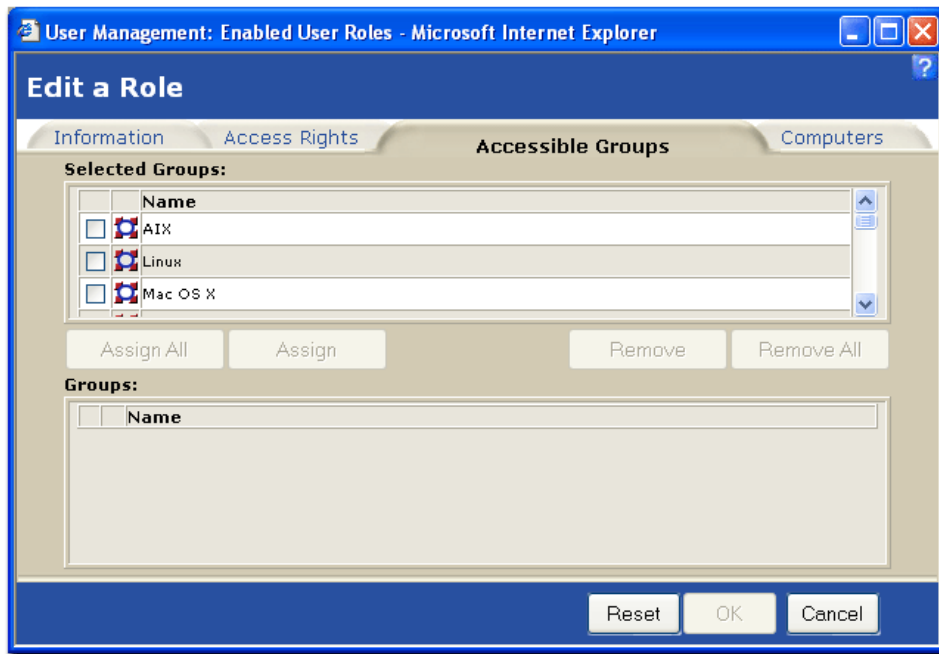
After selecting any number of the access rights listed in the "Access Rights" (lower) pane, click here to assign these rights to the user role.
 - Remove

After selecting any number of the access rights listed in the "Selected Access Rights" (upper) pane, click here to remove these rights from the user role.

- Remove All
Click to remove from the role all of the assigned access rights.
- Information Tab
Select this tab to specify this role's basic information.
- Groups Tab
Select this tab to specify the groups of computers that this role may access.
- Computers Tab
Select this tab to specify individual computers that this role may access.

20.3 Accessible Groups

The Role Property screens allow the PatchLink Administrator to edit a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Groups** screen to specify the groups of computers that this user role may access.



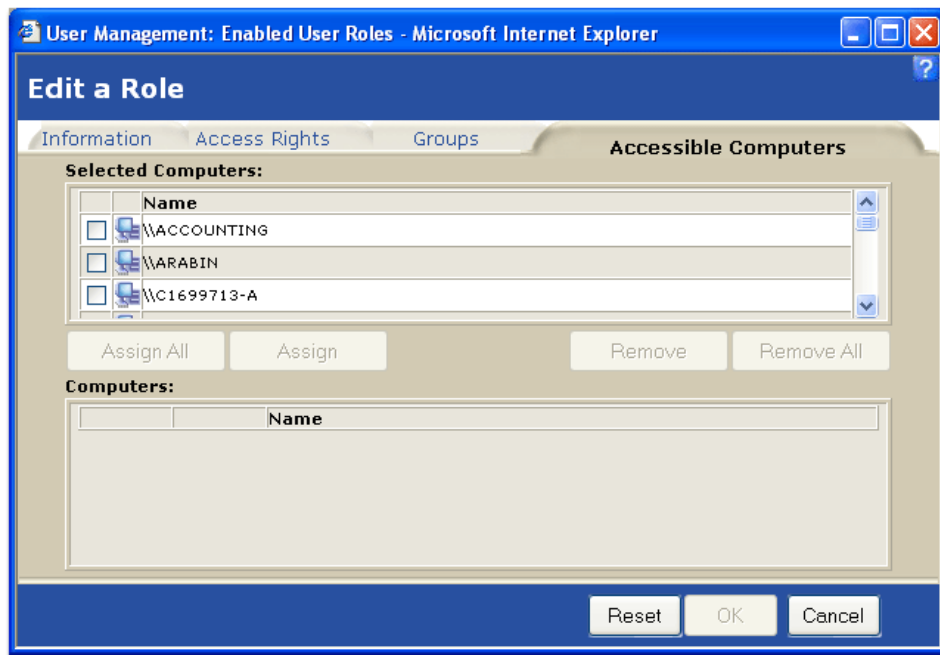
- Accessible Groups Information
 - Selected Groups
A list of the groups of computers that have been assigned to this user role.
 - Groups
A list of all the groups of computers that can be assigned to this user role.

Scroll through and click in the checkbox next to the desired group(s) to initialize and click the **Assign** button. The system populates the **Selected Groups** window with your selections. Use the **Assign All** button to populate the **Selected Groups** with ALL groups from the **Groups** window.

- Screen Functions
 - Assign All
Click to assign all available groups to the user role.
 - Assign
After selecting any number of the groups listed in the "Groups" (lower) pane, click here to assign these groups to the user role.
 - Remove
After selecting any number of the groups listed in the "Selected Groups" (upper) pane, click here to remove these groups from the user role.
 - Remove All
Click here to remove from the role all of the assigned groups.
 - Information Tab
Select this tab to specify this role's basic information.
 - Access Rights Tab
Select this tab to specify this role's access rights to PLUS functionalities.
 - Computers Tab
Select this tab to specify individual computers that this role may access.

20.4 Accessible Computers

The Role Property screens allow the PatchLink Administrator to edit a user role. The role can be assigned access rights to various PLUS functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Computers** screen to specify the individual computers that this user role may access.



- Accessible Computers Information

- Selected Computers

A list of all the computers that have been assigned to this user role.

- Computers

A list of all the computers that can be assigned to this user role.

Scroll through and click in the checkbox next to the desired computer(s) to initialize and click the **Assign** button. The system populates the **Selected Computers** window with your selections. Use the **Assign All** button to populate the **Selected Computers** with ALL computers from the **Computers** window.

- Screen Functions

- Assign All

Click to assign all available computers to the user role.

- Assign

After selecting any number of the computers listed in the "Computers" (lower) pane, click here to assign these computers to the user role.

- Remove

After selecting any number of the computers listed in the "Selected Computers" (upper) pane, click here to remove these computers from the user role.

- Remove All

Click here to remove from the role all of the assigned computers.

- Information Tab
Select this tab to specify this role's basic information.
- Access Rights Tab
Select this tab to specify this role's access rights to PLUS functionalities.
- Groups Tab
Select this tab to specify the groups of computers that this role may access.

Upon closure of the Edit a Role Wizard, the homepage will be refreshed with the newly edited Role.

21. Options

Home | Vulnerabilities | Inventory | Packages | Computers | Groups | Users | Reports | **Options** | Help

The Advanced Configuration Options page displays six main option and configuration views on which PLUS relies on. They are: Subscription Service, Subscription Licenses, PLUS Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

The screenshot shows the 'Options' page in the PatchLink interface. The 'Subscription Service' tab is selected, displaying 'Subscription Service Information' and 'Subscription Service History'.

Subscription Service Information:

- Last Subscription Poll: 8/6/2003 12:10:09 PM
- Subscription Agent Status: Sleeping
- Account ID: 587342A9-810F-4413-814C-2E3BAA1B6625
- Subscription Communication Interval: 1 Day at 03:00 (24-hour)
- Subscription Host URL: https://www.patchlink.com/update/
- Proxy Host: (empty field)

Subscription Service History:

Type	Status	Start Date	Stop Date	Duration	Successful
Licenses	Completed	8/6/2003 12:10:09 PM	8/6/2003 12:10:28 PM	18 (secs)	True
Packages	Completed	8/6/2003 4:06:23 AM	8/6/2003 4:06:26 AM	3 (secs)	True
Reports	Completed	8/6/2003 3:00:03 AM	8/6/2003 4:05:51 AM	65.8 (mins)	True
Packages	Completed	8/6/2003 12:00:17 AM	8/6/2003 12:00:18 AM	2 (secs)	True
Packages	Completed	8/5/2003 1:08:17 PM	8/5/2003 1:08:22 PM	5 (secs)	True
Licenses	Completed	8/5/2003 12:05:08 PM	8/5/2003 12:05:11 PM	3 (secs)	True
Packages	Completed	8/5/2003 10:03:32 AM	8/5/2003 10:03:35 AM	4 (secs)	True
Packages	Completed	8/5/2003 8:47:25 AM	8/5/2003 8:47:26 AM	2 (secs)	True
Packages	Completed	8/5/2003 4:02:49 AM	8/5/2003 4:02:52 AM	3 (secs)	True
Reports	Completed	8/5/2003 3:00:03 AM	8/5/2003 4:02:34 AM	62.5 (mins)	True
Packages	Completed	8/5/2003 12:00:11 AM	8/5/2003 12:00:13 AM	2 (secs)	True
Packages	Completed	8/4/2003 5:40:52 PM	8/4/2003 5:40:54 PM	2 (secs)	True
Packages	Completed	8/4/2003 4:26:06 PM	8/4/2003 4:26:07 PM	1 (secs)	True
Packages	Completed	8/4/2003 4:16:39 PM	8/4/2003 4:16:40 PM	1 (secs)	True
Packages	Completed	8/4/2003 2:58:59 PM	8/4/2003 2:58:59 PM	1 (secs)	True
Packages	Completed	8/4/2003 2:56:36 PM	8/4/2003 2:56:38 PM	1 (secs)	True
Packages	Completed	8/4/2003 2:44:41 PM	8/4/2003 2:44:42 PM	1 (secs)	True
Packages	Completed	8/4/2003 2:37:32 PM	8/4/2003 2:37:33 PM	1 (secs)	True
Packages	Completed	8/4/2003 2:17:19 PM	8/4/2003 2:17:20 PM	2 (secs)	True

21.1 Subscription Service Information

- Subscription Service Information
 - Last Subscription Poll

The date and time of when the subscription agent last contacted the host site for new updates.
 - Subscription Agent Status

The current status of the subscription agent.
 - Account ID

The identification number of your account with the host site. It is created when the PatchLink Update Server first registers itself with the host site.

- Subscription Communication Interval
- The amount of time (number of minutes, hours or days) the subscription agent will wait between contacting the host site. Select the desired time from the drop down menu and select the Save button on the Action Menu to validate the change.
- Subscription Host URL
- The URL (or web address) of the host site.
- Proxy Host
- The proxy host information the subscription agent uses, if it is going through a proxy. Enter the desired proxy information and select the Save button on the Action Menu to validate the change.

- Subscription Service History

This is a history of the tasks the subscription agent has done or is doing. It tells:

- Type
- The *Type* of the agent task.
- Status
- The *Status* of an agent task.
- Start Date
- The *Start Date* is when the task started.
- Stop Date
- The *Stop Date* is when the task was completed.
- Duration
- The *Duration* is how long the task took.
- Successful

Successful is whether or not the task completed successfully or ended in failure.

21.2 Action Menu



- Save
Allows the PatchLink User the ability to save the changes to either the Subscription Communication Interval or Proxy Host.
- Update Now
Allows the PatchLink Administrator the ability to initiate Replication to keep PLUS up to date with the latest Vulnerabilities, Distribution Packages, and Subscription Licenses.
- Export
Allows the PatchLink User the ability to export the Subscription Data to a comma-separated value (CSV) file.

21.3 Subscription Service Security

The Subscription Service tab of the Options section requires the View Options:Subscription Security Access Right. If a user does not have the correct access, the display will automatically redirect the user over to an Options tab that they do have access to. If the user does not have access to any Options tabs, they will receive an access denied error message.

Save requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

Update Now requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

21.4 Subscription Licenses

The Advanced Configuration Options page displays six main option and configuration views on which PLUS relies on. They are: Subscription Service, Subscription Licenses, PLUS Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

The screenshot shows the PatchLink Options page with the 'Subscription Licenses' tab selected. The page header includes navigation links (Home, Reports, Inventory, Packages, Computers, Groups, Users, Options, Help) and the server time (8/6/2003 2:18:55 PM GMT-07:00). The 'Advanced Configuration Options' section contains tabs for Subscription, Subscription Licenses, Defaults, Policies, E-Mail, and Support. The 'License Information' section displays the following data:

Licenses In Use:	10	Total Non-Expired Licenses:	25
Licenses Available:	15		

Purchase Date	Vendor	Effective Date	Expiration	Purchased
11/28/2001 5:00:00 PM	PatchLink Corporation	11/28/2001 5:00:00 PM	12/12/2003 5:00:00 PM	25

At the bottom of the page, there is a 'patchlink' logo and buttons for 'Verify' and 'Export'.

- License Information
 - Licenses In Use

The number of licenses the PatchLink Update Server has in use by registered agents.
 - Licenses Available

The total number of licenses that are left available.
 - Total Non-Expired Licenses

The total number of licenses the PatchLink Update Server that are not expired.

Each time you purchase a license, a license group entry is created that represents that purchase. The list of License Groups are displayed, and for each License Group is shown:

- Purchase Date

The date the license group was purchased.
- Vendor

Tells who the license group was purchased from. The name is also a web link, so by clicking on it, you will be taken to their homepage.

- Effective Date

The date the license group becomes effective.

- Expiration

The date the license group expires.

- Purchased

The amount of licenses purchased.

21.5 Action Menu



- Verify

Allows the PatchLink Administrator the ability to initiate License Replication to keep PLUS up to date with the latest Subscription Licenses.

- Export

Allows the PatchLink User the ability to export the License Data to a comma-separated value (CSV) file.

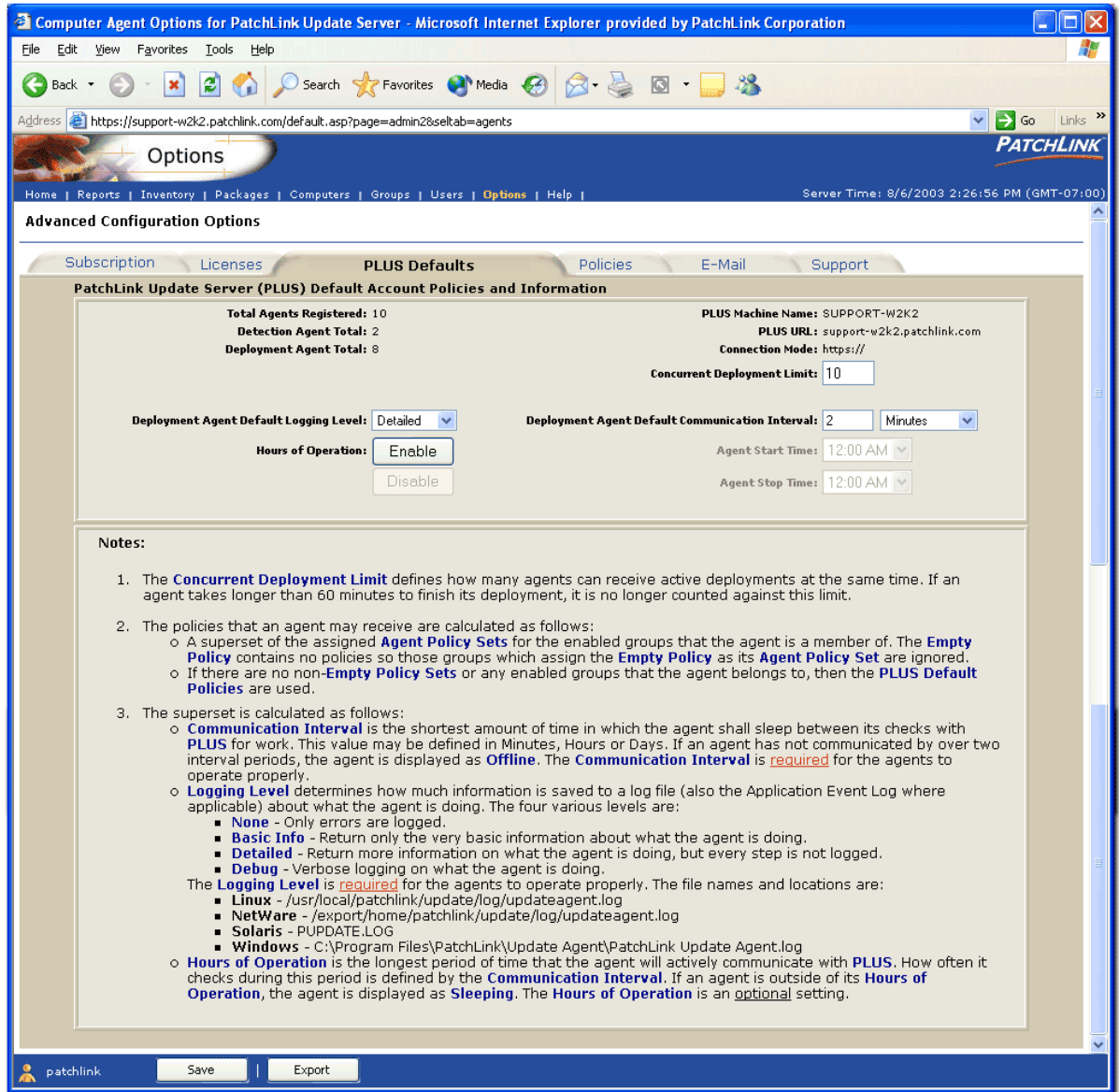
21.6 Subscription License Security

The License tab of the Options section requires the [View Options: Licenses Security Access Right](#). If a user does not have the correct access, hyperlink is disabled.

Export requires the Export Subscription [Data Security Access Right](#). If a user does not have the correct access, the button is disabled.

21.7 PLUS Defaults

The Advanced Configuration Options page displays six main option and configuration views on which PLUS relies on. They are: Subscription Service, Subscription Licenses, PLUS Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.



Computer Agent Options for PatchLink Update Server - Microsoft Internet Explorer provided by PatchLink Corporation

Address: <https://support-w2k2.patchlink.com/default.asp?page=admin2&seltab=agents>

Options

Home | Reports | Inventory | Packages | Computers | Groups | Users | **Options** | Help | Server Time: 8/6/2003 2:26:56 PM (GMT-07:00)

Advanced Configuration Options

Subscription | Licenses | **PLUS Defaults** | Policies | E-Mail | Support

PatchLink Update Server (PLUS) Default Account Policies and Information

Total Agents Registered: 10 Detection Agent Total: 2 Deployment Agent Total: 8	PLUS Machine Name: SUPPORT-W2K2 PLUS URL: support-w2k2.patchlink.com Connection Mode: https:// Concurrent Deployment Limit: 10
---	---

Deployment Agent Default Logging Level: Detailed
Deployment Agent Default Communication Interval: 2 Minutes
Hours of Operation: Enable
 Agent Start Time: 12:00 AM
 Agent Stop Time: 12:00 AM

Notes:

- The **Concurrent Deployment Limit** defines how many agents can receive active deployments at the same time. If an agent takes longer than 60 minutes to finish its deployment, it is no longer counted against this limit.
- The policies that an agent may receive are calculated as follows:
 - A superset of the assigned **Agent Policy Sets** for the enabled groups that the agent is a member of. The **Empty Policy** contains no policies so those groups which assign the **Empty Policy** as its **Agent Policy Set** are ignored.
 - If there are no non-**Empty Policy Sets** or any enabled groups that the agent belongs to, then the **PLUS Default Policies** are used.
- The superset is calculated as follows:
 - Communication Interval** is the shortest amount of time in which the agent shall sleep between its checks with **PLUS** for work. This value may be defined in Minutes, Hours or Days. If an agent has not communicated by over two interval periods, the agent is displayed as **Offline**. The **Communication Interval** is **required** for the agents to operate properly.
 - Logging Level** determines how much information is saved to a log file (also the Application Event Log where applicable) about what the agent is doing. The four various levels are:
 - None** - Only errors are logged.
 - Basic Info** - Return only the very basic information about what the agent is doing.
 - Detailed** - Return more information on what the agent is doing, but every step is not logged.
 - Debug** - Verbose logging on what the agent is doing.
 - The **Logging Level** is **required** for the agents to operate properly. The file names and locations are:
 - Linux** - /usr/local/patchlink/update/log/updateagent.log
 - NetWare** - /export/home/patchlink/update/log/updateagent.log
 - Solaris** - PUPDATE.LOG
 - Windows** - C:\Program Files\PatchLink\Update Agent\PatchLink Update Agent.log
 - Hours of Operation** is the longest period of time that the agent will actively communicate with **PLUS**. How often it checks during this period is defined by the **Communication Interval**. If an agent is outside of its **Hours of Operation**, the agent is displayed as **Sleeping**. The **Hours of Operation** is an **optional** setting.

patchlink Save Export

- PLUS Default Account Policies and Information
 - Total Agents Registered

The total number of agents registered to the PatchLink Update Server Detection Agent Total
 - Detection Agent Total

The total number of detection agents registered to the PatchLink Update Server PLUS Machine Name
 - Deployment Agent Total

The total number of deployment agents registered to the PatchLink Update Server PLUS Machine Name
 - PLUS Machine Name

The name of the computer in which the PatchLink Update Server is installed on.
 - PLUS URL

The URL of the PatchLink Update Server.
 - Connection Mode

The connection mode in which the PatchLink Update Server is acting in. It is either *HTTP://* which is insecure mode, or *HTTPS://*, which is secure mode.
 - Concurrent Deployment Limit

The *concurrent deployment limit* defines how many agents can receive active deployments at the same time. If an agent takes longer than 60 minutes to finish its deployment, it is no longer counted against this limit. The purpose of this limit is to throttle the number of deployments given to agents across the entire PatchLink Update Server (PLUS).
An example of this is the case of multiple deployments being created to run at the same time. Though each may have its own sequential limit of how many agents may perform the deployment at any one time, all of the deployments are running at the same time and this may cause the performance of the server to decrease.
 - Deployment Agent Default Logging Level

The level at which the agent is logging messages about its actions. The various levels are: None, Basic Information, Detailed, Debug.
 - Deployment Agent Default Communication Interval

The amount of time (number of minutes, hours or days) is the length of time the client agent will wait between contacting the PatchLink Update Server.
 - Hours of Operation

Clicking on the Enable button will enable the *Agent Timer*. Start and Stop times can be assigned for the agent to poll the PatchLink Update Server

Clicking on the disable button will disable the *Agent Timer*. The agent will no longer have a start and a stop time. It will start communicating with the PatchLink Update Server as soon as it is assigned this policy and will continue till the policy or the agent is removed.

- Agent Stop Time
The time at which the agent will stop contacting the PatchLink Update Server.
- Agent Start Time
The time at which the agent will start contacting the PatchLink Update Server.

21.8 Action Menu



- Save
Allows the PatchLink Administrator the ability to save License Replication the changes to the PLUS and Agent Defaults.
- Export
Allows the PatchLink User the ability to export the License Data to a comma-separated value (CSV) file.

21.9 PLUS Defaults Security

The Defaults tab of the Options section requires the View Options:Defaults Security Access Right. If a user does not have the correct access, hyperlink is disabled.

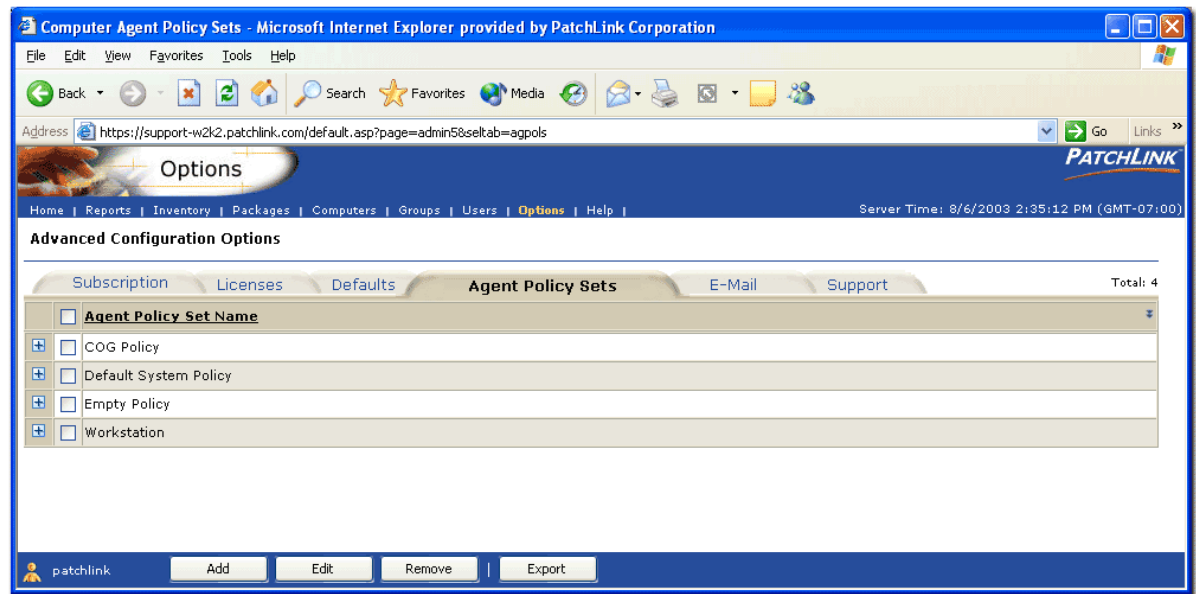
Save requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

21.10 Agent Policy Sets

The Advanced Configuration Options page displays six main option and configuration views on which PLUS relies on. They are: Subscription Service, Subscription Licenses, PLUS Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

A set of constraints that govern the agent features of communication interval, logging level, and the agent start and stop times. An agent policy is associated with a group and is applied to all the members of that group. For every newly created group, the system creates a default agent policy. Click the  to view additional information and statistics about the policy.



- Agent Policy Set Name
 - Policy Name
The name of the policy. There are two types of policies: System and User
 - Policy Type
This indicates whether the policy was created by a user or by the system
 - Trace Level
The logging level that is chosen at the time of Policy generation.
 - Operation Start Time
The time at which the agent will start communicating with the PatchLink Update Server.
 - Operation Stop Time
The time at which the agent will stop communicating with the PatchLink Update server.
 - Description
The description that is entered at the time of Policy generation.
 - Created On
The date and time the policy was created
 - Created By
The user who created the policy
 - Last Modified On
The date and time the policy was last modified
 - Last Modified By
The user who last modified the policy
 - Communication Interval
The amount of time (number of minutes, hours or days) the client agent will wait between contacting the PatchLink Update Server.

21.11 Action Menu



- **Add**
Allows the PatchLink Administrator the ability to create a new Agent Policy Set using the Agent Policy Set Property Page. See [Section 22; Add a Policy Wizard](#) for more information.
- **Edit**
Allows the PatchLink Administrator the ability to edit a selected Agent Policy Set using the Agent Policy Set Property Page. See [Section 23; Edit a Policy Wizard](#) for more information.
- **Remove**
Allows the PatchLink Administrator the ability to delete a selected Agent Policy Set.
- **Export**
Allows the PatchLink User the ability to export the Subscription Data to a comma-separated value (CSV) file.

21.12 Agent Policy Sets Security

The Policies tab of the Options section requires the [View Options: Policies Security Access Right](#). If a user does not have the correct access, hyperlink is disabled.

Export requires the Export [Subscription Data Security Access Right](#). If a user does not have the correct access, the button is disabled.

21.13 Advanced E-Mail Notifications

The Advanced Configuration Options page displays six main option and configuration views on which PLUS relies on. They are: Subscription Service, Subscription Licenses, PLUS Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

Set up PLUS to alert you via email when certain thresholds are reached.

Options

Home | Reports | Inventory | Packages | Computers | Groups | Users | **Options** | Help | Server Time: 8/7/2003 9:18:58 AM (GMT-07:00)

Advanced Configuration Options

Subscription | Licenses | Defaults | Policies | **E-Mail Notification** | Support

Current E-Mail Notifications

	New Reports	New Agent Registrations	Subscription Failure	Deployment Failure	Low System Disk Space	Low Storage Disk Space	Low Available License Count	Up-Coming License Expiration	License Expiration	Notification Address
☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	reneg@patchlink.com

Alert Thresholds SMTP Relay: mail.patchlink.com

Low System Disk Space: Alert When Below 1025 MB Check Disk Space Every 1 Hours	Low Available License Count: Alert When Below 25 Licenses
Low Storage Disk Space: Alert When Below 1000 MB Check Disk Space Every 1 Hours	Up-Coming License Expiration: Alert When Days Remaining Are Below 90

patchlink Add Save Remove Export Test

- **Current E-Mail Notifications**
 - **New Vulnerabilities**
By selecting this notification, you will be sent an e-mail notification each time new vulnerabilities are downloaded via the subscription agent from the host site.
 - **New Agent Registrations**
By selecting this notification, you will be sent an e-mail notification each time a new agent registers up to the PatchLink Update Server.
 - **Subscription Failure**
By selecting this notification, you will be sent an e-mail notification each time the subscription agent task fails.
 - **Deployment Failure**
By selecting this notification, you will be sent an e-mail notification each time a client agent fails at deploying a package.
 - **License Expiration**
By selecting this notification, you will be sent an e-mail notification whenever a license group expires.
 - **Notification Address**
The e-mail addresses that will be notified when any of the following events occur.

- **Alert Thresholds**
 - **Low System Disk Space**

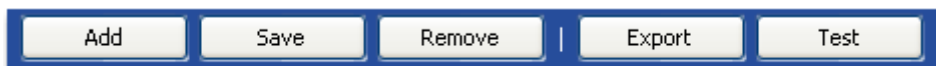
By selecting this notification, you will be sent an e-mail notification whenever the disk space on the system volume goes under this value (in megabytes). Besides an input field to be able to change this value (under the Alert Thresholds section) there is another field which is the Check Disk Space Interval. This value is the amount of time (number of minutes, hours or days) that the PatchLink Update Server will wait between checking the system disk space.
 - **Low Storage Disk Space**

By selecting this notification, you will be sent an e-mail notification whenever the disk space on the storage volume goes under this value (in megabytes). Besides an input field to be able to change this value (under the Alert Thresholds section) there is another field which is the Check Disk Space Interval. This value is the amount of time (number of minutes, hours or days) that the PatchLink Update Server will wait between checking the storage disk space.
 - **Low Available License Count**

By selecting this notification, you will be sent an e-mail notification whenever the license count gets below this value. This value can be changed by changing it in the Alert Thresholds section.
 - **Up-Coming License Expiration**

By selecting this notification, you will be sent an e-mail notification whenever a license group is about to expire within this value (in Days). This value can be changed by changing it in the Alert Threshold section.

21.14 Action Menu



- **Add**

Allows the PatchLink Administrator the ability to add a new e-mail notification entry.
- **Save**

Allows the PatchLink Administrator the ability to save the e-mail notification changes as well as the changes notification alert thresholds.
- **Remove**

Allows the PatchLink Administrator the ability to remove selected e-mail notification entries.
- **Export**

Allows the PatchLink User the ability to export the Subscription Data to a comma-separated value (CSV) file.
- **Test**

Allows the PatchLink Administrator the ability to send a e-mail to a selected e-mail address to verify that e-mails are getting through.

21.15 Advanced E-mail Notifications Security

The E-Mail tab of the Options section requires the [View Options: E-Mail Security Access Right](#). If a user does not have the correct access, hyperlink is disabled.

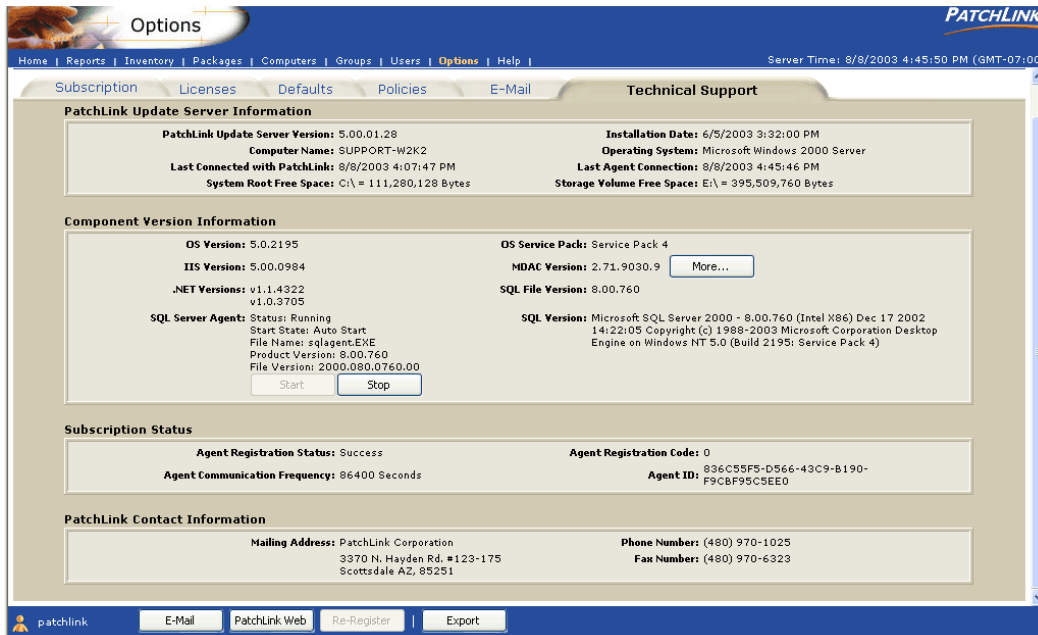
Save requires the [Manage Options Security Access Right](#). If a user does not have the correct access, the button is disabled.

Export requires the [Export Subscription Data Security Access Right](#). If a user does not have the correct access, the button is disabled.

21.16 Technical Support

The Advanced Configuration Options page displays six main option and configuration views on which PLUS relies on. They are: Subscription Service, Subscription Licenses, PLUS Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

View Technical Information about PLUS



- PatchLink Update Server Information
 - PatchLink Update Server Version
The version number of the PatchLink Update Server.
 - Computer Name
The name of the computer, which the PatchLink Update Server was installed on.
 - Last Connected with PatchLink
The last date and time that the subscription agent connected up with the host site.
 - System Root Free Space
The amount of free disk space for the system volume.
 - Installation Date
The date PLUS was installed.
 - Operating System
The operating system that PLUS is running on.
 - Last Agent Connection
The last date and time any agent has connected up with the PatchLink Update Server.
 - Storage Volume Free Space

The amount of free disk space for the storage volume.

- Component Version Information
 - OS Version
The extra operating system information.
 - IIS Version
The version number of the IIS web server.
 - .NET Version
The version number of the .NET Framework(s) installed on the server
 - SQL Server Agent: Clicking the Start / Stop button will start or stop the SQL Server Agent.
Displays the following:
 - The current status
 - The start up state
 - SQL Agent Filename
 - Product Version number
 - File Version number
 - OS Service Pack
The service pack information about the operating system.
 - MDAC Version
The version number of MDAC. Click on the MDAC to view all of the MDAC component version numbers.
 - SQL File Version
The version number of the SQL Server File: SQLServer.exe.
 - SQL Version
The SQL Server version information.
- Subscription Status
 - Agent Registration Status
The status of the registration process for the subscription agent against the host site.
 - Agent Registration Code
The status code number for the registration status message.
 - Agent Communication Frequency
The amount of time (number of minutes, hours or days) is the length of time the subscription agent will wait between contacting the host site.
 - Agent ID
The ID number given to the subscription agent upon registration by the host site.
- PatchLink Contact Information
 - Mailing Address
 - Phone Number
 - Fax Number

21.17 Action Menu



- **E-Mail**
Allows the PatchLink User the initiate an e-mail, using the user's default e-mail client, to a select number of PatchLink Departments.
- **PatchLink Web**
Allows the PatchLink User to instantly bring up the PatchLink Update Technical Support web site.
- **Re-Register**
Allows the PatchLink Administrator the ability to initiate the process to register (or re-register) the PLUS Subscription Agent against PLHOST. This button is only available when the Subscription Agent has not successfully registered against PLHOST.
- **Export**
Allows the PatchLink User the ability to export the Subscription Data to a comma-separated value (CSV) file.

21.18 Technical Support Security

The Support tab of the Options section requires the [View Options: Support Info Security Access Right](#). If a user does not have the correct access, hyperlink is disabled.

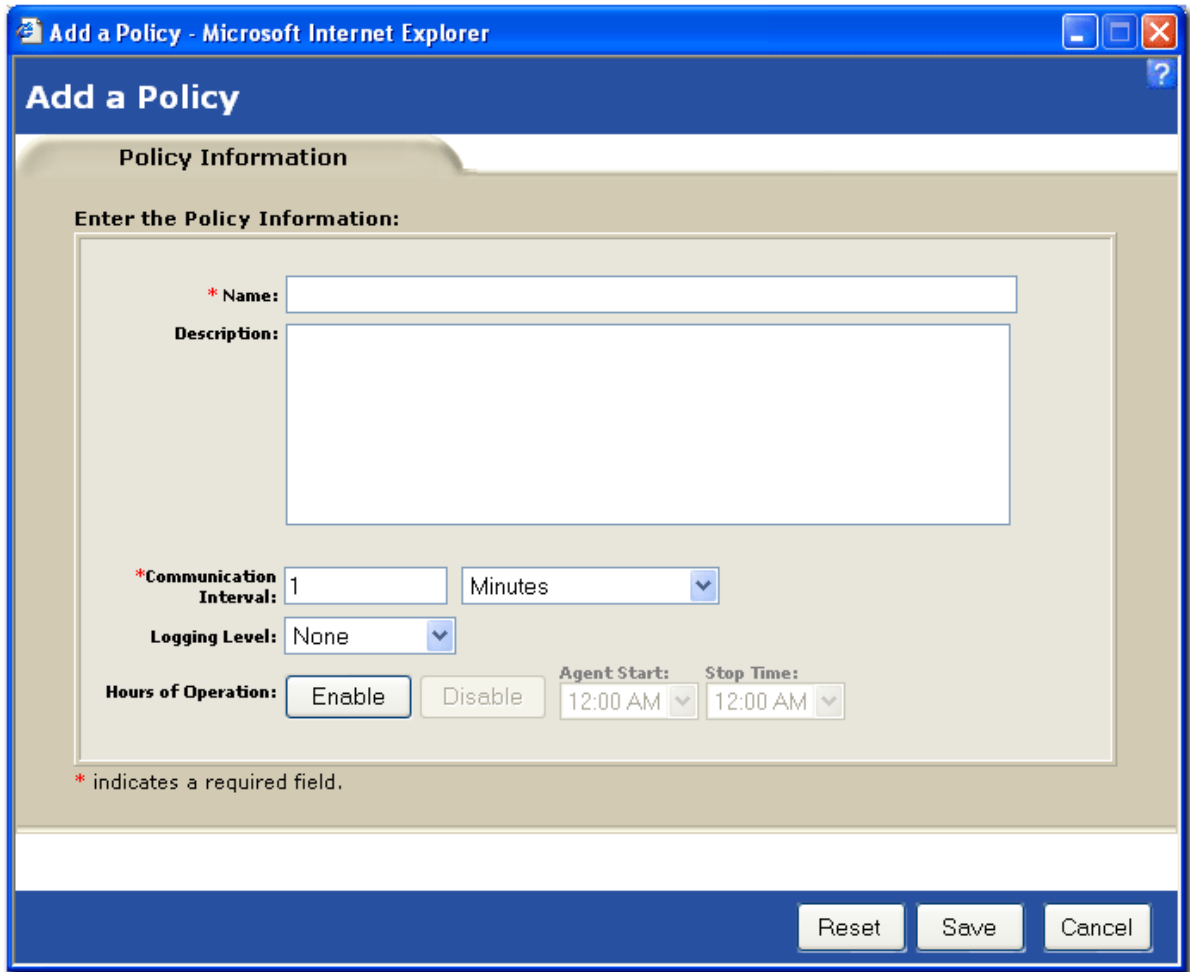
Export requires the [Export Subscription Data Security Access Right](#). If a user does not have the correct access, the button is disabled.

22. Add a Policy Wizard

This wizard allows you to create and add a policy to the PatchLink Update Server. You can specify the policy attributes by entering data in the fields of the wizard.

Go to the **Options** homepage and select the **Agent Policy Sets** tab. Click on the **Add** button to add a on the Action Menu. This will initialize the **Add a Policy** Wizard.

22.1 Policy Information



Add a Policy - Microsoft Internet Explorer

Add a Policy

Policy Information

Enter the Policy Information:

* Name:

Description:

*Communication Interval: Minutes

Logging Level: None

Hours of Operation: Enable Disable Agent Start: 12:00 AM Stop Time: 12:00 AM

* indicates a required field.

Reset Save Cancel

- Name
Input a Name for your Policy (required)
- Description
Add a Description of your Policy (optional)
 - Enter in the desired Communication interval: The amount of time (number of minutes, hours or days) is the length of time the client agent will wait between contacting the PatchLink Update Server.
 - Enter in the desired Logging Level: The level at which the agent is logging messages about its actions. The various levels are:
 - None
 - Basic Information
 - Detailed
 - Debug
- Hours of Operation
Clicking on the Enable button will enable the Agent Timer. Start and Stop times can be assigned for the agent to poll the PatchLink Update Server

Clicking on the button will disable the Agent Timer. The agent will no longer have a start and a stop time. It will start communicating with the PatchLink Update Server as soon as it is assigned this policy and will continue till the policy or the agent is removed.

Agent Stop Time: The time at which the agent will stop contacting the PatchLink Update Server.

Agent Start Time: The time at which the agent will start contacting the PatchLink Update Server.

22.2 Page Functions

- Save
Saves the field values that you manually entered
- Cancel
Exits the wizard and does not save any changes to the field values.
- Reset
Resets the field values to their original state

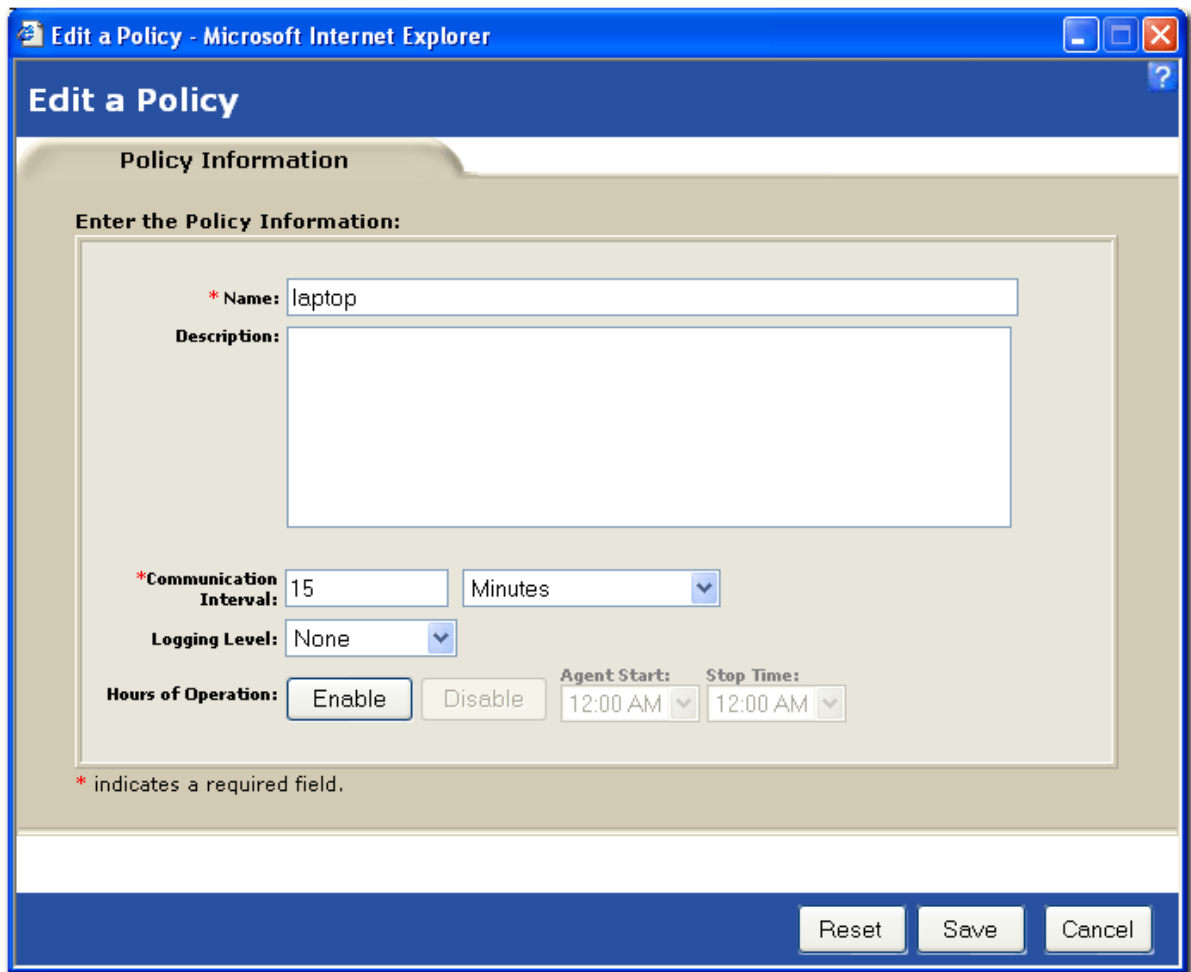
Upon refreshing the Options homepage, the Policy will be added and appears under the Agent Policy Set Name

23. Edit a Policy Wizard

This wizard allows you to change the attributes of an existing policy set. You can edit and specify the policy attributes by entering data in the fields of the wizard.

Go to the **Options** homepage, select the **Agent Policy Sets** tab, and select the policy that you wish to edit by clicking in the checkbox next to that specific policy. Click on the Edit button on the Action Menu. This will initialize the **Edit a Policy** Wizard.

23.1 Policy Information



Edit a Policy

Policy Information

Enter the Policy Information:

* Name:

Description:

* Communication Interval:

Logging Level:

Hours of Operation:

Agent Start: Stop Time:

* Indicates a required field.

- Name
Edit the Name for your Policy
- Description
Edit the Description of your Policy
 - Enter in the desired Communication interval: The amount of time (number of minutes, hours or days) is the length of time the client agent will wait between contacting the PatchLink Update Server.
 - Enter in the desired Logging Level: The level at which the agent is logging messages about its actions. The various levels are:
 - None
 - Basic Information
 - Detailed
 - Debug
- Hours of Operation
Clicking on the Enable button will enable the Agent Timer. Start and Stop times can be assigned for the agent to poll the PatchLink Update Server

Clicking on the button will disable the Agent Timer. The agent will no longer have a start and a stop time. It will start communicating with the PatchLink Update Server as soon as it is assigned this policy and will continue till the policy or the agent is removed.

Agent Stop Time: The time at which the agent will stop contacting the PatchLink Update Server.

Agent Start Time: The time at which the agent will start contacting the PatchLink Update Server.

23.2 Page Functions

- Save
Saves the field values that you manually entered.
- Cancel
Exits the wizard and does not save any changes to the field values.
- Reset
Resets the field values to their original state.

Upon refreshing the Options homepage, the edited Policy will be added and appears under the Agent Policy Set Name.

24. Hardening the PLUS

Steps that can be taken to harden a PatchLink Update Server

There are a few steps that can be taken to harden a PatchLink Update Server that is to be put on the public Internet. You can opt to implement some or all of these suggestions, and these are of course just guidelines:

24.1 INSTALL YOUR SERVER WITH SSL:

Purchase a valid certificate from Verisign, Entrust, Thawte etc for your IIS web server, and use it with PatchLink Update. This process just involves installing your .CER certificate file before rebooting after the main filecopy phase of the installation. The advantage is that with an SSL certificate installed, all agent communication and all administration is now fully encrypted - and so there is no way to spoof or snoop communications on the wire.

24.2 TURN OFF NON-CRITICAL SERVICES:

Microsoft Windows2000 ships with all the features turned on. There are a number of services you may wish to turn off (eg: RPC, Remote Registry, etc) to reduce the risk of hacker attacks. PatchLink doesn't encourage this type of lockdown - we would suggest using port blocking or a firewall instead, however if you are careful this can be an effective approach.

The following are *required* services to run PatchLink Update:

- wwwpublishing
- IIS Admin Service
- Mssqlserver
- Sqlserver agent
- PatchLink Update

24.3 REMOVE YOUR SERVER FROM THE DOMAIN:

You probably don't have your machine in a corporate domain if it is out on the Internet! For safety's sake you should have as few people being able to login to the server as possible - just use local accounts.

24.4 USE SECURE PASSWORDS:

Worm attacks frequently try to log in with weak / commonly used passwords (letmein, no password, etc) so please don't use them. For an Internet secure password we would recommend DOD standard 12 characters with alpha, numeric, punctuation and mixed case characters all being represented in your password.

24.5 TURN OFF WINDOWS NETWORKING:

Click on My Network Places, Select "Properties" from its popup menu, Choose the "Local Area Connection", Select "Properties" from its popup menu. This will show you the "Local Area Connection Properties" ... the properties of your main network card (there may be multiple network cards in your server). Go ahead and select "File and Printer Sharing for Microsoft Networks" and push the "Uninstall" button to remove MS file & print network service. NOTE: do NOT uninstall the "Client for Microsoft Networks" as it is required by MS SQL Server and MS Internet Information Server.

24.6 LOCK OFF ALL BUT THE REQUIRED TCP/IP PORTS:

Within "Local Area Connection Properties" window, select "Internet Protocol

TCP/IP" and push the "Properties" button. On the Properties dialog, push the "Advanced..." button, then click the "Options" tab, select "TCP/IP filtering" and push the "Properties" button. You are now able to set specific port filters for your computer, so that you can 'firewall' off all but the ports that you need:

- => Check the "Enable TCP/IP Filtering" checkbox
- => Select the "Permit Only" TCP Ports button
 - Add port number 443
 - Add port number 80 (not needed if you followed step 1)
 - No other ports are required, though you may want to allow DNS out, maybe TS or VNC
- => Select the "Permit Only" UDP Ports button
 - No UDP ports are required, leave this section blank

Once you save these settings and reboot your server, your machine will now be fully isolated from TCP/IP access except through HTTP/HTTPS. If you lock out everything except port 80/port 443, you will also have to add an entry to your HOSTS file in the `\winnt\system32\drivers\etc` directory so that your server can get to www.patchlink.com to pick up its patch subscription:

206.124.169.50 www.patchlink.com
216.205.112.66 storage12.patchlink.com

24.7 PUT YOUR UPDATE SERVER BEHIND A FIREWALL:

Since the PLUS software pulls its patch updates from the subscription servers, there is no need to allow access from the Internet to the PLUS server. Be sure to allow access to both subscription servers through your firewall from the internal network to the Internet on the following ports:

https://www.patchlink.com	206.124.169.50	Port 443
https://storage12.patchlink.com	216.205.112.66	Port 443

This is normally an easier alternative to (6), however if your company does not have a hardware or software firewall, you can use method (6) to get the same level of network isolation.

24.8 APPLY THE MSDE SQL PATCHES:

Apply these patches so you don't get the SLAMMER worm on your server, apply the most recent applicable patches for IIS, SQL, and the Operating System.

25. PLUS Reference

25.1 PLUS Security

There are multiple layers to security for PatchLink Update:

- Web Site Authentication
 - Web Site Encryption via SLL
 - User (Security) Roles
-
- Web Site Authentication
Internet Information Services (IIS) controls authentication in to the PLUS web site, which means the operating system itself is validating users and their passwords when they log in to the site. Control of who has access and who does not, at this level, is controlled by a local user group.
 - Web Site Encryption via SSL
SSL provides an encrypted wrapper around all web communication to and from the product. Since all communication is over the web, this means by installing PLUS in to SSL mode and then adding an SSL certificate to the PLUS web site will provide a wall around customer's data, away from prying eyes.
 - User (Security) Roles
Every feature, page and action throughout PLUS has been assigned to a series of Access Rights. Combining these access rights + together form a user role. Roles also contain a list of groups and computers (which do not belong to the list of groups). Put this all together and PLUS now contains a mechanism in which regardless of how you authenticated in to the PLUS web application, what you can do is defined solely by your PatchLink Administrator. If a user does not have a User Role, or it is disabled, and their access immediately is denied to everything.

25.2 Error Pages

The PatchLink Update Server provides four distinct error pages. These pages are:

- Insufficient Browser Capabilities
This page is displayed whenever a user visits the PatchLink Update Server with a browser incapable of properly processing the site. The minimum browser requirements are provided on this page, along with links to download the latest versions of popular browsers.
- Requested Page Not Found
This page is displayed whenever a user attempts to navigate to a address that does not exist on the PatchLink Update Server. Links are provided to common sections of the PatchLink Update Server to assist the user in returning to the site.
- Login Failure
This page is displayed whenever a user fails to provide valid credentials for access to the PatchLink Update Server.

- System Component Version Conflict

This page is display whenever a system component version conflict is detected. The system components of the PatchLink Update Server are checked every time a user logs into the site. If a conflict is detected, this page is displayed providing the component(s) that failed to meet the required version. The PatchLink Update Server also attempts to notify the system administrator via email of the conflict.

26. Programmer's Reference

Programmer's reference gives you some samples and examples of the coding necessary to perform advanced functions on PLUS.

26.1 PLCCAgent Script Object

The Agent scripting host contains the imbedded object *PLCCAgent*. This object provides quick functions to the Windows Registry, Agent Environment, and Output.

26.2 PLCCAgent GetOSVersion Method

The **GetOSVersion** function obtains information about the version of the operating system that is currently running.

- Syntax
object.**GetOSVersion** (strOS, iMajor, iMinor, iBuild, strServicePack)
- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>strOS</i>	Win95, Win98, WinME, WinNT, Win2K, WinXP
<i>iMajor</i>	Major version (NT 4.0 Major = 4)
<i>iMinor</i>	Minor Version
<i>iBuild</i>	Build Number
<i>strServicePack</i>	Service Pack Number

- Example
PLCCAgent.GetOSVersion szOS, iMajor, iMinor, iBuild, szPS

26.3 PLCCAgent GetPolicy Method

- Description
The **GetPolicy** function obtains the value for an agent policy.
- Syntax
object.**GetPolicy** (strName, strValue)
- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>strName</i>	"Interval", "IntervalType", "TraceLevel"
<i>strValue</i>	Returned value of a policy

26.4 PLCCAgent InitiateSystemShutdown Method

- Description
Used to restart machine.
- Syntax
object.**InitiateSystemShutdown**
- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.

- Remarks
Causes the machine to restart. See Window SDK API [ExitWindowsEx](#) 

26.5 PLCCAgent PollHost Method

- Description
The **PollHost** function tells the agent to poll the host as soon as this package containing this script completes.
- Syntax
object.**PollHost** ()

- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.

26.6 PLCCAgent RegCloseKey Method

- Syntax
`object.RegCloseKey( hKey )`

- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>hKey</i>	Handle to open key

- Return
Returns non zero value if successful.
- Example
If PLCCAgent.RegOpenKey(0, "HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey) then
 ' Key opened successfully
 PLCCAgent.CloseKey(hKey)
End if

26.7 PLCCAgent RegEnumKey Method

- Description
The **RegEnumKey** function enumerates subkeys of the specified open registry key.
The function retrieves the name of one subkey each time it is called.
- Syntax
`object. RegEnumKey ( hKey, strEnumKey, iIndex )`

- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>hKey</i>	Handle to an open registry key.
<i>strEnumKey</i>	A variable that receives the name of the subkey in string form. This function copies only the name of the subkey, not the full key hierarchy.
<i>iIndex</i>	Specifies the index of the subkey to retrieve. This value should be zero for the first call to the RegEnumKey function and then incremented for subsequent calls

- Return

Returns non zero value if successful.

- Remarks

To enumerate subkeys, an application should initially call the **RegEnumKey** function with the *iIndex* parameter set to zero. The application should then increment the *iIndex* parameter and call the **RegEnumKey** function until there are no more subkeys (until the function returns 0). While an application is using the **RegEnumKey** function, it should not make calls to any registry functions that might change the key being queried.

- Example

```
If PLCCAgent.RegOpenKey( 0, "HKLM\Software\Microsoft\Windows\CurrentVersion",  
hKey ) then  
    iKeyIndex = 0 ' Must start with 0  
    do while PLCCAgent.RegEnumKey( hKey, szKey, iKeyIndex )  
        PLCCAgent.Write "Key = " & szKey & vbcrLf  
        iKeyIndex = iKeyIndex + 1 'Next Key  
    loop  
    PLCCAgent.CloseKey( hKey )  
End If
```

26.8 PLCCAgent RegEnumValue Method

- Description

The **RegEnumValue** function enumerates the values for the specified open registry key. The function copies one indexed value name and data block for the key each time it is called.

- Syntax

object.**RegEnumValue**(hKey, strEnumValue, iIndex)

- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>hKey</i>	Handle to an open registry key.
<i>strEnumValue</i>	A variable that receives the value name in string form.
<i>iIndex</i>	Specifies the index of the value to retrieve. This value should be zero for the first call to the RegEnumValue function and then incremented for subsequent calls

- Return

Returns non zero value if successful.

- Remarks

To enumerate *values*, an application should initially call the **RegEnumValue** function with the *iIndex* parameter set to zero. The application must increment the *iIndex* parameter and call the **RegEnumValue** function until there are no more *values* (until the function returns 0).

- Example

```
' Read all Values from a Key and output them to the Host
If PLCCAgent.RegOpenKey( 0, "HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey ) then
  iKeyValue = 0 ' Must start with 0
  do while PLCCAgent.RegEnumValue( hKey, szValue, iValueIndex )
    PLCCAgent.Write "Value = " & szValue & vbcrLf;
    iKeyValue = iKeyValue + 1 'Next Value
  loop
  PLCCAgent.CloseKey(hKey )
End if
```

26.9 PLCCAgent RegOpenKey Method

- Description
Returns the registry value named by *strName*.
- Syntax
object. **RegOpenKey**(hRootKey, strKey, strValue)
- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>hRootKey</i>	Handle to previous open key (0=none)
<i>strKey</i>	Key name to open.
<i>hRetKey</i>	Return Handle to open key.

- Return
Returns non zero value if successful.
- Remarks
If *hRootKey* is 0, *StrName* must begin with one of following root key names .
Otherwise, this key must be a subkey of the key identified by the *hRootKey* parameter. The **RegOpenKey** function uses the default security access mask to open a key.

Root Key Name	Description
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE
HKCR	HKEY_CLASSES_ROOT

- Example
If PLCCAgent.RegOpenKey(0, "HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey) then
 ' Key opened successfully
End if
PLCCAgent RegQueryValue Method

26.10 PLCCAgent RegRead Method

- Description
Returns the registry value named by *strName*.
- Syntax
object.**RegRead**(strName, strValue, iType)
- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>strName</i>	Value name to read.
<i>strValue</i>	Data read from registry.
<i>iType</i>	An Integer variable that receives a code indicating the type of data stored in the specified value. 1 = REG_SZ, 2 = REG_EXPAND_SZ, 4 = REG_DWORD

- Remarks
StrName must begin with one of following root key names:

Root Key Name	Description
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE
HKCR	HKEY_CLASSES_ROOT

The **RegRead** method supports only REG_SZ, REG_EXPAND_SZ, REG_DWORD and REG_BINARY data types. If the registry has other data types, **RegRead** returns 0.

- Example
The following example reads a value from the registry:

```
Dim Value
if ( PLCCAgent.ReadReg (
    "HKLM\Software\Microsoft\Windows\CurrentVersion\ProductId", Value, Type ) then
    PLCCAgent.Write "The Product is " & Value & vbCrLf
endif
```

26.11 PLCCAgent RegSetValue Method

- Description
The **RegSetValue** function sets the data and type of a specified value under a registry key.
- Syntax
object.**RegSetValue**
- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>hKey</i>	Handle to an open registry key.
<i>strSubKey</i>	A string containing the name of the value to set.
<i>Type</i>	A code indicating how the data is to be stored. 1 = REG_SZ, 2 = REG_EXPAND_SZ, 4 = REG_DWORD < /FONT >
<i>Value</i>	Variable that contains the data to set in the registry. If an Integer variable is a VarType of vbInteger and the Type is set to 1 (REG_SZ) then the value will be converted to a decimal string and stored as a REG_SZ. The same holds true for a string stored as an Integer.

- Return
Returns non zero value if successful.
- Remarks
All variables in VBScript/JScript are Variant in nature(meaning the variable could represent any type from integers, strings, to arrays); therefore, conversion of data types could yield undesirable results. If storing an Integer (REG_DWORD) try passing an Integer variable.
- Example
If PLCCAgent.RegOpenKey(0, "HKLM\Software\Microsoft\Windows\CurrentVersion", hKey) then
Value = "This is a string"
Type = 1 ' 1 = String or REG_SZ
PLCCAgent.RegSetValue(hKey, "Test", Value, Type)
PLCCAgent.CloseKey(hKey)
End if

26.12 PLCCAgent SetReturnCode Method

- Description
The **SetReturnCode** function is use to alter the package status. If during a PreScript or PostScript execution the script decides that this package has not accomplished its task, it may set a return code and a description of what went wrong.
If set return code is used in the pre-script the package files will not be downloaded and the error returned to the host.

- Syntax
`object.SetReturnCode ( iRc, strRCDescription )`

- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>iRC</i>	A return code. Range must be from 1-255
<i>strRCDescription</i>	A string description of the return code

- Example
`PLCCAgent.SetReturnCode 1,"This install didn't work!"`

26.13 PLCCAgent Write Method

- Description
Used to return data to the Host Server.

- Syntax
`object.Write(output)`

- Parameters

Parameter	Description
<i>object</i>	PLCCAgent object.
<i>output</i>	String data to be sent to Host

- Remarks
Output can be vbString, vbInteger, or vbLong. vbInteger and vbLong are converted to string prior to send.
The agent supports two different scripts, Pre-Script and Postscript. Therefore two output streams will be received by the Host for each script.

Note: There is currently no user interface provided at the host to view the contents of this stream. A future version may provide a user and/or programmatic interface to this stream.

- Example
PLCCAgent.Write "Hello World" & vbCrLf

27. Glossary

Terms, definitions and definitions for terminology used throughout the PatchLink Update Server.

Agent

A software routine that resides in the background and waits to perform an action when a specified event occurs.

Agent Policies

An agent's behavior is defined by its policies. The three main policies are:

- Hours of Operation
- Communication Interval
- Logging Level

Though the policies can be overridden locally on the computer via the PatchLink Update Control Panel Applet, they will be reset whenever the policies are changed by the PatchLink Administrator on PLUS.

ATL Controls

ATL (Active Template Library, formerly called ActiveX Template Library) is a Microsoft program library (set of prepackaged program routines) for use when creating Active Server Page (ASP) code and other ActiveX program components with C++ (including Visual C++) that runs in a browser to enhance the user experience.

Authentication

The act of verifying that a user has access to a system or function of a software application running on the web server.

Authenticode

Authenticode is a technology based on industry standards that provides a method for developers to digitally sign their code (.EXE, .CAB, .OCX, and .CLASS files). When code is signed, the company signing the code vouches that the code is safe and free of viruses, and takes responsibility for the code.

Browser

Application software that allows the user to access and view documents on the Internet or World Wide Web.

Code Signing

The process of digitally signing programs for verification purposes.

Control Panel Applet

PatchLink provides an applet found in the Control Panel that allows easy interaction with the PatchLink Update Agents. The Action menu in applicable sections allows this interaction. See the Action Menu in each section for applicability.

Client

In relation to Agent-to-Client language, a client is used in reference to, and may also be, a computer, node, server, or system.

Client Agent (aka Deployment Agent)

The Client Agent is a service running on the computer that performs two primary tasks: 1) communicates with PLUS and gathers its updated agent policies and deployments to perform

and 2) executes those deployments then sends the results back to PLUS. Since this service is required to run all the time, its behavior is defined by agent policies set by the PatchLink Administrator on PLUS.

Cross Platform

Open interfaces now allow some programs to run on different platforms (operating systems) or to interoperate with different platforms through mediating programs.

Detection Agent (aka Discovery Agent)

The Detection Agent is executed either by a user manually from the client computer or automatically by the deployment agent when the Discover Applicable Updates (DAU) System Task is the next deployment for the Client Agent to perform. The DAU task is responsible for the discovery and vulnerability analysis on the computer. The Detection Agent sends its system information and inventory to the PLUS and, based on this information, PLUS determines which vulnerabilities are applicable to the computer and the patch status of each vulnerability.

DHCP

Dynamic Host Configuration Protocol is a protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network.

Discovery Agent

Provides both hardware and software information about a computer on which the Update Agent has been installed. There is no requirement to install the discovery agent, as it will be automatically deployed as needed by the Update Server.

DNS Names

The domain name system (DNS) is the way that Internet domain names are located and translated into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

FTP

File Transfer Protocol, a standard protocol, is the simplest way to exchange files between computers on the Internet. (IETF/W3C RFC959)

Host Name

The server computer name that typically is the DNS name (e.g., www.patchlink.com).

HTTP

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. (IETF/W3C RFC2616)

HTTPS

HTTPS Secure Hypertext Transfer Protocol is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned via HTTP over SSL by the Web server.

IIS

Internet Information Server is a group of Internet servers (Web or HTTP, FTP, and Gopher) and other capabilities for Microsoft's Windows NT Server operating system.

IP

Internet Protocol is the network transmission standard for Internet communication.

LDAP

Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.

MSDE

Microsoft Data Engine is an enabling technology that provides local data storage and is completely compatible with the Microsoft SQL Server(tm) version 7.0 code base. This technology transforms Access from a simple file-server database application into an extremely powerful and highly scalable client-server solution for any size organization.

OSD

Open Software Distribution is an Extensible Markup Language (XML) grammar. It creates a standard way to describe software components -- their versions, their underlying structure and their relationships to other components. This is the standard for using the Internet for automatic software updates.

Password

A unique code entered with the User Name to access a computer on a network or a particular function of a software application.

PatchLink Administrator

Any user who is assigned any of the PLUS access rights which control the functionality of PLUS or its deployments is considered a PatchLink Administrator. This is not to be confused with the PatchLink Super-User, who is assigned the Administrator user role.

PatchLink Super-User

Any number of users can be assigned the Administrator user role and thus can be called a PatchLink Super-User.

PatchLink User

Any user who has access to authenticate in to PLUS is considered a PatchLink User.

PLHOST

PLHOST is an acronym for the **P**atchLink **U**ppdate **H**ost **S**erver. PLUS obtains its subscription of patches from these central repositories where vulnerabilities and their associated packages are located.

PLUS

PLUS is an acronym for the **P**atch**L**ink **U**ppdate **S**erver. PLUS allows users to be able to determine what vulnerabilities are not patched on their networks.

Port

Number A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

Proxy Server

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Server

A computer that provides file sharing and various other servers between many users and computers on a network.

SQL Server

A trademark for a Microsoft database server that utilizes SQL. SQL Server is a popular database management system for Windows NT environments.

SSL

Secure Sockets Layer is a program layer created by Netscape for managing the security of message transmissions in a network.

TCP/IP

Transmission Control Protocol/Internet Protocol is the basic communication language or protocol of the Internet.

UDP

User Datagram Protocol is a communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).

Update Agent Software

that is installed on computers which enable PatchLink Update to distribute files and software onto those computers.

User Name

A unique name for access purposes assigned to a user of a computer on a network.

User Role

A user role contains a chosen set of PatchLink access rights and computers and/or groups on which those access rights may pertain to. There are four system user role templates a PatchLink Administrator may use to create custom user roles that fit in a more precise manner with the security policies of an organization. When a user role is assigned to a PatchLink User, that user now has access to view certain pages, perform certain functions on the assigned computers and/or groups.

Verisign Certificate

VeriSign, Inc, provides Internet-based trust services needed by websites, enterprises and individuals to conduct secure communications and electronic commerce on-line. A VeriSign certificate is issued after a person's or company's identity is verified and enables them to digitally sign programs that run in a browser, or to prove authenticity of a given web site address.

Vulnerability

A breach from the original design, concept or intended behavior of a computer's hardware or software which leaves the computer, or any piece of it, in an exposed state. Malicious users can use this to force other unattended actions to be performed. Vulnerabilities are often caused by defects or bugs, though this is not always the case. Many times the very configuration may result in unexpected exposures. Even out of date documentation may be labeled as a vulnerability as un-informing a user of how to perform actions in the preferred manner may result in systems being widely exposed.

Vulnerability

A series of signatures designed to determine whether a computer is applicable to the vulnerability. Once a computer has been determined that it is applicable to a given vulnerability, the vulnerability fingerprints determine the patch status of the computer.

Vulnerability Analysis

The results for a given (or all) vulnerabilities.

Web Server

A program that publishes content using the HTTP protocol so that it can be viewed using any type of compliant browser from any location on the connected Intranet or Internet.

X.500

An acronym for CCITT Directory Services Protocol that is an industry standard for directory information contents.

XML

eXtensible Markup Language is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

28. Revision History

Version	Revision Date	Change Description	Author
1.1	01/02/2004	Initial Document	S. Newton
1.2	01/05/2004	Added New 5.1 Features: Agent Management Center	S. Newton
1.3	01/06/2004	Revised Screen Shots	S. Newton
1.4	04/04/2004	Section 3.2.5 Advanced Page Search, Filtering, and View Saving language and graphics added. Section 4.6 PatchLink Update Server Status Page section (language and graphics) added. Section 5 Vulnerability Reports Homepage Screenshot Updated Section 5.4.2 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Section 6 Inventory Homepage Screenshot Updated Section 6.1.2 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Section 7 Packages Homepage Screenshot Updated Section 7.2.2 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Section 9.3.1 Note Added Section 9.5 Deployment Options section added. Section 10 Computers Homepage Screenshot Updated Section 10.3.2 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Section 11 Groups Homepage Screenshot Updated Section 11.2.2 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Section 11.14.2 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Section 11.19.1 Advanced Page Search, Filtering, and View Saving section (language and graphics) added. Various Sections: Formatting corrections. Various Sections: Style Updates. Various Sections: Multiple Screenshot Updates. Section 23 Revisions added	J. Bentley
1.5	05/31/04	Section 2 What's new in PL version 6.0? - Revised language to reflect 6.0 changes instead of 5.1. Section 3.5 "Agents and Installing Them" updated. Section 3.6 Agent Management Center added Section 10.4 Action Menu; Added AMC Reference and PatchLink Distribution Point Advanced Section 27 Revisions added Various Sections: Updated Section References to reflect the true sections, need to verify Various Sections: Grammar, punctuation.	J. Bentley
1.6	06/02/04	Updated AMC Screenshots New Template applied to document	Craig Burton J. Bentley
1.8	08/04/04	Changed all Reports references to "Vulnerabilities"	Jill Burkett